# Google Cloud VPN Interop Guide

Using Cloud VPN With Fortinet® FortiGate 300C



Fortinet<sup>®</sup>, FortiGate, and other Fortinet marks are trademarks of Fortinet, Inc., its subsidiaries and affiliates.

# Contents

Introduction **Environment Overview** Topology **Preparation** Overview **Getting Started IPsec Parameters** Policy Based IPsec VPN **Configuration - GCP UI Configuration - GCP CLI** Create the VPN Gateway Configuration - Fortinet FortiGate 300C: CLI **IPsec Configuration** Create the Phase 1 Configuration Create the Phase 2 Configuration **Firewall Policy** Create the Address Objects Create the Address Groups **Create the Firewall Policies** Configuration - Fortinet FortiGate 300C: GUI **IPsec Configuration Firewall Policy** Route Based IPsec VPN IPsec VPN Using Cloud Router **Configuration - Google Cloud Router UI Cloud Router VPN Tunnel Configuration - Google Cloud Router CLI** Create the VPN Gateway Reserve a Static IP Create the Cloud Router Create the VPN Tunnel Add the BGP Link Local Interface Add the BGP Peering Session Configuration - Fortinet FortiGate 300C: CLI Interface Configuration Configure the Tunnel Interface **IPsec Configuration** Create the Phase 1 Configuration Create the Phase 2 Configuration

Configure BGP Routing Configuration - Fortinet FortiGate 300C: GUI IPsec Configuration Tunnel Interface BGP Testing the Site-to-Site VPN Verify Connectivity Testing the Tunnel Basic Ping

## Introduction

This guide walks you through the process of configuring the Fortinet 300C for integration with the <u>Google Cloud VPN service</u>. 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:	Fortinet
Model:	FortiGate 300C
Firmware Rev:	04000022
Software Rev:	v5.2.7, build 718 (GA)

## Topology

This guide will describe three VPN topologies.

- 1. A site-to-site policy based IPsec VPN tunnel configuration using static routing
- 2. A site-to-site route based IPsec VPN tunnel configuration
- 3. A site-to-site IPsec VPN tunnel configuration using the Google Cloud Router and BGP



## 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 Fortinet FortiGate for use with the Google cloud VPN service is to ensure that the following prerequisite conditions have been met:

- Fortinet FortiGate online and functional with no faults detected
- Admin access to the Fortinet FortiGate
- At least one configured and verified functional internal interface
- One configured and verified functional external interface

## **IPsec Parameters**

For the Fortinet FortiGate 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

Phase	Cipher Role	Cipher
Phase 1	Encryption	aes-256
	Integrity	aes256-sha1
	prf	sha1-96
	Diffie-Hellman (DH)	Group 15
	Phase 1 lifetime	36,000 seconds (10 hours)
Phase 2	Encryption	aes-cbc-256
	Integrity	aes256-sha1

#### The IPsec configuration used in this guide is specified below:

## Policy Based IPsec VPN

## Configuration - GCP UI

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:



All parameters needed to create a new VPN connection are entered on this page. A detailed description of each parameter is provided below:

-	Google Cloud Platfo	۹ مربع
-	Networking	Create a VPN connection
	Networks	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 proc.
5	External IP addresses	Google Compute Engine VPN gateway (2)
3	Firewall rules	Name 💿
2	Routes	gcp-to-fg300c
	Lond balancian	Description (Optional)
•	Eoad balancing	Google Cloud VPN to Fortinet FortiGate 300C
!	Cloud DNS	
	VPN	Network @
•	Cloud Routers	UTab .
		Region @
		us-bentian +
		IP address 🛞
		Remote peer IP address 💿
		Remote peer IP address 🚱
		209.119.81.228
		IKE version 🛞
		IKEv2 *
		Shared secret @
		MySharedSecret
		Routing options
		Static Dynamic (BGP)
		Static Dynamic (BGP) Remote network IP range @ Enter multiple IP addreases by pressing Return after each one
		Static     Dynamic (BGP)       Remote network IP range:     @       Enter multiple IP addresses by pressing Return after each one       192.168.0.0/24 ×     192.168.2.0/24 ×
		Static     Dynamic (BGP)       Remote network IP range:     @       Enter multiple IP addresses by pressing Return after each one       192.168.0.0/24 ×     192.168.1.0/24 ×       Local subnetworks:     @ (Optional)
		Static     Dynamic (BGP)       Remote network IP range:     @       Enter multiple IP addresses by pressing Return after each one       192.168.0.0/24 ×     192.168.2.0/24 ×       Local subnetworks:     @ (Optional)       1 selected *
		Static     Dynamic (BGP)       Remote network IP ranges     @       Enter multiple IP addresses by pressing Return after each one       192.168.0.0/24 ×     192.168.1.0/24 ×       Local subnetworks     @ (Optional)       1 selected *       Local IP ranges
		Static     Dynamic (BGP)       Remote network IP ranges     Image: Constraint of the state
		Static Dynamic (BBP) Remote network IP ranges Enter multiple IP addresses by pressing Return after each one 192.168.0.0/24 × 192.168.2.0/24 × 192.168.1.0/24 × Local subnetworks @ (Optional) 1 selected * Local IP ranges @ 10.240.0.0/16 × + Add tunnel

The following parameters are required for the VPN gateway:

- Name: the name of the VPN gateway.
- **Description:** a brief description of the VPN connection.
- **Network:** the GCP network the VPN gateway will attach to. **Note:** this is the network to which VPN connectivity will be made available.
- **Region:** the home region of the VPN gateway. **Note:** the VPN gateway must be in the same region as the subnetworks it is connecting.
- **IP address:** the static public IP address which will be used by the VPN gateway. An existing, unused, static public IP address within the project can be assigned, or a new one can be created.

The following parameters are required for each Tunnel which will be managed by the VPN gateway:

- **Remote peer IP address:** the public IP address of the on premises VPN appliance which will be used to connect to Cloud VPN.
- IKE version: the IKE protocol version. This guide assumes IKEv2
- **Shared secret:** a shared secret used for mutual authentication by the VPN gateways. The on-premises VPN gateway tunnel entry should be configured it the same shared secret.
- **Routing options:** Cloud VPN supports multiple routing options for the exchange of route information between the VPN gateways. For this example **static routing** is being used. Cloud Router and BGP are covered <u>later in this guide</u>.
- **Remote network IP ranges:** the on-premises CIDR blocks being connected to GCP via the VPN gateway.
- Local subnetworks: the GCP CIDR blocks being connected to on-premises via the VPN gateway.
- Local IP ranges: the GCP IP ranges matching the selected subnet

## Configuration - GCP CLI

Cloud VPN can also be configured using the <u>gcloud command line tool</u>. Command line configuration requires two steps. First the VPN Gateway is created, then the tunnels are created referring to the VPN Gateway.

#### Create the VPN Gateway

```
gcloud compute target-vpn-gateways create gcp-to-fg300c --network to-lab --region us-central1
```

#### Create the VPN Tunnel

```
gcloud compute vpn-tunnels create my-tunnel --shared-secret MySharedSecret
--peer-address on-prem-IP --target-vpn-gateway gcp-to-fg300c
--local-traffic-selector gcp-CIDR --remote-traffic-selector on-prem-CIDR
```

## Configuration - Fortinet FortiGate 300C: CLI

**IPsec Configuration** 

```
Create the Phase 1 Configuration
config vpn ipsec phase1-interface
    edit "GCP"
        set interface "port1"
        set ike-version 2
        set keylife 36000
        set proposal aes256-sha1
        set comments "VPN: GCP (Created by VPN wizard)"
        set dhgrp 15
        set remote-gw 146.148.68.246
        set psksecret ENC
wDfCX7ikIVbjhh9+DAaX0rCO8x/gnuaFu/yl/flQKuh0SLUURBbG7ITM7MQ+y6TG3ZzUxNWIRlruDPZlgNcqCi
/VEEk5S/vx0DHI81UCBkNz0i1JK7rRdlCQoMepvw+hSU79BlfIPAI2oi7xt+6a6uGYPB3Eszweeqw/YCYQtfyE
+fPGl1NQYcMbkXpa5tBeN6VTLg==
    next
end
Create the Phase 2 Configuration
config vpn ipsec phase2-interface
    edit "Lab_1"
        set phase1name "GCP"
        set proposal aes256-sha1
        set dhgrp 15
       set replay enable
        set keylifeseconds 10800
        set src-subnet 192.168.1.0 255.255.255.0
        set dst-subnet 10.240.0.0 255.255.0.0
   next
    edit "Lab 0"
        set phase1name "GCP"
        set proposal aes256-sha1
        set dhgrp 15
       set replay enable
        set keylifeseconds 10800
        set src-subnet 192.168.0.0 255.255.255.0
        set dst-subnet 10.240.0.0 255.255.0.0
   next
    edit "Lab_2"
        set phase1name "GCP"
        set proposal aes256-sha1
        set dhgrp 15
```

```
set replay enable
set keylifeseconds 10800
set src-subnet 192.168.2.0 255.255.255.0
set dst-subnet 10.240.0.0 255.255.0.0
next
end
```

**Firewall Policy** 

Create the Address Objects

For **remote** subnet entries, substitute the Google Cloud Platform network subnet. For **local** subnet entries, substitute the local 300C subnets:

```
config firewall address
   edit "GCP_remote_subnet_1"
       set uuid 97d79d28-0d99-51e6-8561-1a312ce9ba71
        set subnet 10.240.0.0 255.255.0.0
   next
   edit "GCP_local_subnet_2"
        set uuid 97987828-0d99-51e6-3690-6c658de88669
       set subnet 192.168.2.0 255.255.255.0
   next
   edit "GCP_local_subnet_1"
       set uuid e989f17c-0da6-51e6-1722-80cb52bd4c01
       set subnet 192.168.1.0 255.255.255.0
   next
    edit "GCP_local_subnet_0"
       set uuid f5a5ab0e-0da6-51e6-098d-30320f324a0c
       set subnet 192.168.0.0 255.255.255.0
   next
end
```

Create the Address Groups

Create groups for the local and remote address objects created above:

```
config firewall addrgrp
edit "GCP_local"
set uuid 979d18b0-0d99-51e6-d282-83ea3a020898
set member "GCP_local_subnet_2" "GCP_local_subnet_0" "GCP_local_subnet_1"
set comment "VPN: GCP (Created by VPN wizard)"
next
edit "GCP_remote"
set uuid 97dc53a4-0d99-51e6-4728-b7b8405649e1
set member "GCP_remote_subnet_1"
set comment "VPN: GCP (Created by VPN wizard)"
next
End
```

Create the Firewall Policies

Create two firewall policies, one for Google Cloud Platform network ingress to the 300C local subnets, and one for 300C local subnet egress to the Google Cloud Platform network:

```
config firewall policy
    edit 3
        set uuid 97df898e-0d99-51e6-ff7b-2e266549c953
        set srcintf "port2"
       set dstintf "GCP"
        set srcaddr "GCP_local"
       set dstaddr "GCP_remote"
        set action accept
        set schedule "always"
        set service "ALL"
        set logtraffic all
        set comments "VPN: GCP (Created by VPN wizard)"
   next
    edit 4
        set uuid 97e2f15a-0d99-51e6-b260-bbe2fc82b4bf
        set srcintf "GCP"
        set dstintf "port2"
        set srcaddr "GCP_remote"
        set dstaddr "GCP_local"
        set action accept
        set schedule "always"
        set service "ALL"
        set logtraffic all
        set comments "VPN: GCP (Created by VPN wizard)"
   next
```

end

## Configuration - Fortinet FortiGate 300C: GUI

## **IPsec Configuration**

Login to the Fortinet device using a web browser:



From the VPN configuration option, choose Tunnels to set up a new VPN connection and select "Custom VPN Tunnel (No Template)" from the wizard:

FORTINET FortiGat	e 300C	210 Wizard	Video	() Help	Logout
System	VPN Creation Wizard				
Router					
Policy & Objects	1 VPN Setup				
Security Profiles	Name				
VPN	Template				
B A IPsec	Dialup - FortiClient (Windows, Mac OS, Android)				
- • Wizard	🔣 Site to Site - FortiGate				
Tunnel Templates	Dialup - IOS (Native)				
SSL     Monitor	Dialup - Android (Native L2TP/IPsec)				
	Dialup - Cisco Firewall				
	Site to Site - Clsco				
	Custom VPN Tunnel (No Template)				
	< Back Next> Cancel				
User & Device					
WiFi Controller					
Log & Report					

Populate the VPN Tunnel configuration **Network** section as pictured below:

Remote Gateway: select "Static IP Address"

IP Address: enter the IP address of the Google Cloud VPN Gateway

Interface: select the public interface of the Fortinet device

Dead Peer Detection: select this checkbox to enable DPD

FortiGate 300C				Wizard	Video	Help
			Edit VPN Tunnel			
Name	GCP					
Commente	VPN: GCP (Created by VPN wizar	d)				
Comments		10				
Network			<pre>XX</pre>			
IP Version	IPv4					
Remote Gatewa	y Static IP Address	•				
IP Address	146.148.68.246					
Interface	port1 (outside)	•				
Mode Config						
NAT Traversal						
Dead Peer Dete	tion 🕑					
Authenticati	n on Method : Pre-shared Key		✓ Edit			
IKE Version	: 2					
Phase 1 Prot	osal		✓ Edit			
Algorithms	AECOEG CUAL					
Diffic-Holla	AES250-SHAT					
Diffic field	an oroup : 15					
Phase 2 Sele	tors					
Name	Local Address	Remote Address	© Add			
Lab_0	192.168.0.0/255.255.255.0 10	240.0.0/255.255.0.0				
Lab_2	192.168.2.0/255.255.255.0 10	.240.0.0/255.255.0.0	1 1			
			OK Cancel			

Populate the VPN Tunnel configuration Authentication section as pictured below:

**Method**: for the authentication method select "Pre-Shared Key" **Pre-Shared-Key**: enter the pre-shared key you have chosen to use **IKE**: select IKE version 2

FORTINET FortiGat	e 300C	10 Wizard	Video	(2) Help	
System	Edit VPN Tunnel				j
Router Policy & Objects Security Profiles VPN	Name     GCP       Comments     VPH: GCP (Created by VPH wizard)       Network     VEdit       Remote Gateway : Static IP Address , Interface : pott1				
<ul> <li>■ Tunnels</li> <li>■ Wizard</li> <li>■ Tunnel Templates</li> <li>              ∰ SSL      </li> <li>             ∰ Monitor         </li> </ul>	Authentication               X             Method             Pre-shared Key             Pre-shared Key             Inscrept Second Seco				
4	Phase 1 Proposal     ✓ Edit       Algorithms: AES256.SHA1     Diffie-Hellman Group: 15				
	Name         Local Address         Remote Address         QAdd           Lab_0         192.166.0/255.255.255.255.0         10.240.0.0/255.255.0.0         / 11           Lab_1         192.166.0/255.255.255.0         10.240.0.0/255.255.0.0         / 11           Lab_2         192.166.2.0/255.255.255.0         10.240.0.0/255.255.0.0         / 11				
	OK Cancel				
User & Device WiFi Controller					
Log & Report					

Populate the VPN Tunnel configuration Phase 1 Proposal section as pictured below:

FORTIDET	FortiGate 300C	 10 Witard	STO VIGeo Help
System	Edit VPN Tunnel		
Router Policy & Objects Security Profiles VPN	Name GCP Comments VPN: GCP (Created by VPN wizard)		
🖻 🐴 IPsec	Remote Gateway : Static IP Address , Interface : port1		
Tunnels     Wizard     Tunnel Templat     SSL     Monitor	Authentication Method : Pre-shared Key IKE Version : 2		
	Phase 1 Proposal         Add           Encryption         AE5256 *         Authentication         SHA1 *           Diffie-Hellman Group         1 2         20         19         18         17         16           Local ID         2 15         1 4         5         2         1         16           Phase 2 Selectors         Name         Local Address         Remote Address         0 Add           Lab_0         192.168.00/255.255.0         10.240.00/255.255.0         0 Add		
	Lab_2 192.168.2.0/255.255.0 10.240.0.0/255.255.0.0 / 1		
User & Device WiFi Controller Log & Report			

Populate the VPN Tunnel configuration Phase 2 Proposal section as pictured below:



The completed tunnel configuration will appear as below:

FORTINET FortiGat	te 300C					310 Wizard	Video	() Help	Logout
System				Edit VP	N Tunnel				
Router Policy & Objects Security Profiles	Name Comments	GCP VPN: GCP (Created by V	PN wizard)						
VPN	Network Remote Gateway	: Static IP Address , Interf	ace : port1	/ Edit					
- Wilson - Wizard - Tunnel Templates - 20 SSL - Portals	Authentication Authentication M IKE Version : 2	ethod : Pre-shared Key		/ Edit					
Settings     Monitor     SSL-VPN Monitor	Phase 1 Proposal Algorithms : AES2 Diffie-Hellman G	256-SHA1 roup : 15		/ Edit					
	Phase 2 Selectors           Name           Lab_0         192.1           Lab_1         192.1           Lab_2         192.1	Local Address 68.0.0/255.255.255.0 68.1.0/255.255.255.0 68.2.0/255.255.255.0	Remote Address 10.240.0.0/255.255.0.0 10.240.0.0/255.255.0.0 10.240.0.0/255.255.0.0	bbAQ 全 合 合 合					
				ОК	Cancel				
User & Device									
WiFi Controller									
Log & Report									

## Firewall Policy

First, from the **Policy & Objects** configuration section, under **Objects**, select **Addresses** and create a new **Address** entry for each subnet (local subnets and remote GCP subnets):

FURTINET For	rtiGate 300C		SIO MO CO Wizard Video Help Logout
System		Edit Address	
Router Policy A Objects  Policy Policy Policy Policy Policy Policy Structure	Name Type Subtret / IP Range Interface Show in Address List Comments	SCP_local_sobret_0         1P/Netmask         19:168.0.0/255.255.05.0         any         Image: Comparison of the solution of the solu	
VPN			
User & Device			
WiFi Controller			
Log & Report			

Add all **Address** entries to the appropriate **Address Group** where the entries representing local subnets are added to a local group, and the entries representing GCP subnets (remote) are added to a remote group:

FORTINET Forti	Gate 300C				14 25 35 Wi	tard Video	? Help	Logout
System				Edit Address Group				
Router Policy & Objects	Group Name Show in Address List	GCP_local						
Policy - • IPv4 - • DoS	Members Comments	GCP_local_subnet_0 VPN: GCP (Created by VPN wizard)	× 🕹 32/255					
<ul> <li>Prov Options</li> <li>\$SUSH inspection</li> <li>\$Services</li> <li>\$Services</li> <li>\$Schules</li> <li>Traffic Supers</li> <li>Virtual Ps</li> <li>Virtual Ps</li> <li>Pools</li> <li>\$Monitor</li> </ul>				OK Cancel				
Security Profiles								
VPN								
User & Device								
Log & Report								

#### The completed **Addresses** configuration will appear as below:

	tiGate 300C				Tizard Video	P Logou
System	🔘 Create New 🔻 🖉 Edit 🍵 Delete			By Category O Alphabetically	Q Search	
Router	Name	Туре	Details	Interface	Visibility	Ref. Q
Policy & Objects	Address (7)					
Policy & Objects	GCP_local_subnet_0	Subnet	192.168.0.0/24	Any	0	1
Policy & Objects	GCP_local_subnet_1	Subnet	192.168.1.0/24	Any	0	1
-= IPv4	GCP_local_subnet_2	Subnet	192.168.2.0/24	Any	0	1
- • DoS	GCP_remote_subnet_1	Subnet	10.240.0.0/16	Any	0	1
- * Proxy Options	E SSLVPN_TUNNEL_ADDR1	IP Range	10.212.134.200 - 10.212.134.210	Any	0	2
SSL/SSH Inspection	😑 all	Subnet	0.0.0.0/0	Any	9	0
😑 🛄 Objects	🖸 none	Subnet	0.0.0/32	Any	0	0
Addresses	Address Group (2)					
Services     Schedules	GCP_local 3 Members	Address Group	GCP_local_subnet_2 GCP_local_subnet_0 GCP_local_subnet_1		0	2
Traffic Shapers	GCP_remote	Address Group	GCP_remote_subnet_1		9	2
Security Profiles						
User & Device						
WiFi Controller						
Log & Report						
Log a Report						

Next, from the **Policy & Objects** configuration section, under **Policy**, select **IPv4** and create new firewall **Policy** entries for ingress and egress:

Incoming Interface: originating interface (inside for egress, outside for ingress) Source Address: address group created in the prior section (local or remote) Outgoing Interface: exit interface (inside for egress, outside for ingress) Destination Address: address group created in the prior section (local or remote) Schedule: Always (or limit if required) Service: All (or limit if required)

Action: ACCEPT

FORTINET For	rtiGate 300C			Wizard	Video	() Help	Logout
System			Edit Policy				^
System     Router     Policy & Objects     Policy & Objects     Policy     Policy	Incoming Interface Source Address Source User(s) Source Device Type Outgoing Interface Destination Address Schedule Service Action Firewall / Network Options	portz (inside)         @ GCP_local         Click to add         Click to add         GCP         @ GCP_remote         @ always         @ ALL         ✔ ACCEPT					
	Security Profiles and AntiVrus and Application Control and IPS and SSL/SSH Inspection	default default default default certificate-inspection	3 3 3 3 3 3 3 3 3 3 3				
	Traffic Shaping orn: Shared Shaper orn: Reverse Shaper orn: Per-IP Shaper Logging Options	guarantee-100kbps guarantee-100kbps Click to set					
Security Profiles VPN User & Device WiFi Controller Log & Report	cost Dog Allowed Traffic     Security Events     All Sessions     Capture Packets     Comments     Comments     Com Enable this policy	VPN: GCP (Created by VPN wizard)	32/1023				

After completion there should be two policies, one for ingress and one for egress:

FORTIDET	FortiGate 3	00C									Wizard Video	Help Logout
System	O Cr	eate New 🏼 🖉 Edit 📲	Delete						Section	View 🖲 Global View	Q Search	
Router	Seq.#	T From	т То	T Source	T Destination	V Schedule	T Service	T Action	T NAT	▼ Log	T Co	unt 🗘
Policy & Objects	1	port2 (inside)	GCP	GCP_local	GCP_remote	🧿 always	ALL	✓ ACCEPT	🕲 Disable	() All	35 Packet	s / 2.01 KB
Policy	2	GCP	port2 (inside)	GCP_remote	GCP_local	o always	KALL	✓ ACCEPT	C Disable	All	1,653 Packe	ts / 157.23 KB
- IPv4	3	any	any	🗏 all	🗏 all	🥘 always	S ALL	Ø DENY		🕃 Disable		
Security Profiles												
VPN												
User & Device												
WiFi Controller												
Log & Report					<b>H I</b>	/ 1 🕨 🕅 [ Tota	al: 3 ]					

Route Based IPsec VPN

## **IPsec VPN Using Cloud Router**

## Configuration - Google Cloud Router UI

Google Cloud Router enables dynamic <u>Border Gateway Protocol (BGP)</u> route updates between your Google Cloud Platform network and your on-premise network. For the initial release, Cloud Router supports BGP for <u>Cloud VPN</u> only. Cloud Router works with both legacy networks and <u>Subnetworks</u>.

#### **Cloud Router**

The first step in configuring the Google Cloud Platform for site-to-site VPN connectivity utilizing BGP and the Google Cloud Router is to create a new cloud router. From the Developer Console, select **Networking** and then **Cloud Routers**. From the workspace select **Create Router**:

	Google Cloud Platform		
s √°	Networking	Cloud Routers	
22	Networks		
먭	External IP addresses		
88	Firewall rules		Networking
>\$	Routes		Cloud Routers
A	Load balancing		Google Cloud Router enables dynamic route updates between your
里	Cloud DNS		Compute Engine VPN and your non-Google network. Cloud Router eliminates the need to configure static routes and automatically
53	VPN		discovers network topology changes. Learn more
-	Cloud Routers		create router

All parameters needed to create a new cloud router are entered on this page. A detailed description of each parameter is provided below:

	Google Cloud Platfor	m <b>२</b>	
~	Networking	← Create a cloud router	
	Networks External IP addresses Firewall rules Routes Load balancing Cloud DNS	A cloud router direct traffic between your Compute Engine VPN gateways, remote VPN gateways, or another Compute Engine VPN gateways.           Name         Image: Compute Engine VPN gateways           gcp-to-fg300c-router         Image: Cloud Router Instance for gcp-to-fg300c VPN           Network         Image: Cloud Router Instance for gcp-to-fg300c VPN	
5	VPN	to-fg300c	•
*	Cloud Routers	Region  us-central1  Google ASN  65500  Create Cancel	•

- Name: the name of the cloud router.
- **Description:** a brief description of the cloud router.
- **Network:** the GCP network the cloud router will attach to. **Note:** this is the network on route information will be managed.
- **Region:** the home region of the cloud router. **Note:** the cloud router must be in the same region as the subnetworks it is connecting.
- **Google ASN**: the BGP Autonomous System Number assigned to the cloud router. Use any private ASN (64512 65534, 420000000 4294967294) not in use elsewhere in the network

The newly created instance will appear in the list of Cloud Routers. Click **Configure** under VPN Gateway to create the VPN tunnel:

	Google Cloud Platform			۹					
Ż	Networking	Cloud Routers	+ CRE	ATE ROUTER	T DELET	E			
8	Networks	Name A	Network	Region	Google ASN	VPN Gateway	VPN tunnels	BGP sessions	Logs
C <sup>e</sup>	External IP addresses	gcp-to-fg300c-router	to-fg300c	us-central1	65500	Configure			View
88	Firewall rules								
×\$	Routes								
A	Load balancing								
<b>9</b>	Cloud DNS								
5	VPN								
***	Cloud Routers								

### **VPN** Tunnel

All parameters needed to create a new VPN connection are entered on this page. A detailed description of each parameter is provided below:

	Google Cloud Platform	n Q
< V	Networking	← Create a VPN connection
8	Networks	A virtual private network lets you securely connect your Google Comute Engine
먭	External IP addresses	establish the IPSec connectivity. Learn more
RR	Firewall rules	Google Compute Engine VPN gateway 📀
	2	Name 📀
74	Routes	gcp-to-fortinet-fg300c
A	Load balancing	Description (Optional)
里	Cloud DNS	Google Cloud VPN to Fortinet Fortigate 300C
92	VPN	Network
+**	Cloud Routers	to-fg300c 👻
		Region @
		us-central1
		IP address
		gcp-to-vpn-test1 (146.148.68.246)
		Tunnels 😡
		Tunnels     Image: Constraint of the state o
		Tunnels       Image: State of the state of
		Tunnels       Image: State of the state of
		Tunnels       Image: State of the state of
		Tunnels       Image: State of the state of
		Tunnels       Image: Constraint of the start of the star
		Tunnels       Image: Static       Dynamic (BGP)         You can have multiple tunnels to a single Peer VPN gateway         Remote peer IP address       Image: Static         209.119.81.228       Image: Static       Image: Static         NysharedSecret       Image: Static       Image: Static         Shared secret       Image: Static       Image: Static         Static       Dynamic (BGP)       Image: Static
		Tunnels You can have multiple tunnels to a single Peer VPN gateway Remote peer IP address
		Tunnels       Image: Constraint of the standard of the
		Tunnels       Image: Constraint of the standard of the
		Tunnels       Image: Solution of the state
		Tunnels       Image: Solution of the state

The following parameters are required for the VPN gateway:

- Name: the name of the VPN gateway.
- **Description:** a brief description of the VPN connection.
- **Network:** the GCP network the VPN gateway will attach to. **Note:** this is the network to which VPN connectivity will be made available.
- **Region:** the home region of the VPN gateway. **Note:** the VPN gateway must be in the same region as the subnetworks it is connecting.
- **IP address:** the static public IP address which will be used by the VPN gateway. An existing, unused, static public IP address within the project can be assigned, or a new one can be created.

The following parameters are required for each Tunnel which will be managed by the VPN gateway:

• **Remote peer IP address:** the public IP address of the on premises VPN appliance which will be used to connect to Cloud VPN.

- IKE version: the IKE protocol version. This guide assumes IKEv2
- Shared secret: a shared secret used for mutual authentication by the VPN gateways. The on-premises VPN gateway tunnel entry should be configured it the same shared secret.
- **Routing options:** Cloud VPN supports multiple routing options for the exchange of route information between the VPN gateways. For this example **Dynamic (BGP)** is being used. Static Routes were covered <u>earlier in this guide</u>.
- **Cloud Router:** the Cloud Router instance associated with this VPN tunnel created in the <u>Cloud Router section</u>.
- **BGP session:** the BGP configuration to be used by the Cloud Router for this VPN tunnel. Click the pencil to create a new configuration:

gcp-to-fortinet-fg300c-bgp	
Peer ASN 🔞	
65501	
Google BGP IP address 🔞	Peer BGP IP address 💿
169.254.0.1	169.254.0.2

The following parameters are required to configure the BGP session:

- Name: the name of the BGP session
- Peer ASN: the unique BGP ASN of the on-premises router
- **Google BGP IP address, Peer BGP IP address:** The Google BGP IP and Peer BGP IP must be link-local in the same /30 subnet. Make sure they aren't the network or broadcast address of the subnet.

Once all of the BGP session info has been entered, click **Save and continue** to complete, then click **Create** on the Create a VPN connection form to create the VPN connection.

## **Configuration - Google Cloud Router CLI**

Cloud VPN can also be configured using the <u>gcloud command line tool</u>. Command line configuration requires multiple steps.

#### Create the VPN Gateway

Create the VPN gateway. Make note of the chosen name (**my-gateway**), network and region for use in future steps:

gcloud compute target-vpn-gateways create **my-gateway** --project **my-project** --network **my-network** --region **my-region** 

### Reserve a Static IP

Reserve a static IP address in the Google Cloud Platform network and region where the VPN gateway was created. Make a note of the created address for use in future steps.

gcloud compute addresses create vpn-static-ip --project **my-project** --region **my-region** 

#### Create the Cloud Router

Create a Cloud Router in the region where the VPN gateway was created. This example uses ASN 65001 for the Cloud Router ASN, but any private ASN (64512 - 65534, 4200000000 - 4294967294) not already in use in the peer network can be used:

```
gcloud beta compute --project my-project routers create my-router --region my-region
--network my-network --asn my-asn
```

### Create the VPN Tunnel

Create the VPN tunnel referencing the **VPN gateway** and **Cloud Router** created earlier. Make note of the chosen tunnel name for use in future steps. The **peer-address** should be set to the outside interface IP of the Fortinet device and a **shared-secret** should be set which will be used later in configuring the Fortinet side of the tunnel.

```
gcloud beta compute --project my-project vpn-tunnels create my-tunnel --region
my-region --ike-version 2 --target-vpn-gateway my-gateway --peer-address my-IP
--shared-secret my-PSK --router my-router
```

#### Add the BGP Link Local Interface

Update the Cloud Router config to add a virtual interface (--interface-name) for the BGP peer. The BGP interface IP address must be a link-local IP address belonging to the IP address range 169.254.0.0/16 and it must belong to same subnet as the interface address of the peer router. The netmask length is recommended to be 30. Make sure each tunnel has a unique pair of IPs. Alternatively, if --ip-address and --mask-length are blank, and --peer-ip-address in the next step is left blank, the IP addresses will be automatically generated:

```
gcloud beta compute --project my-project routers add-interface my-router
--interface-name my-if --ip-address my-link-local-IP --mask-length 30 --vpn-tunnel
my-tunnel --region my-region
```

### Add the BGP Peering Session

Update the Cloud Router config to add the BGP peer to the interface. This example uses ASN 65002 for the peer ASN. Any public ASN or private ASN (64512 - 65534, 420000000 - 4294967294) not already in use in the peer network can be used. The BGP peer interface IP address must be a link-local IP address belonging to the IP address range 169.254.0.0/16. It must belong to same subnet as the Google Cloud Platform-side interface. Make sure each tunnel has a unique pair of IPs.

gcloud beta compute --project **my-project** routers add-bgp-peer **my-router** --peer-name bgp-peer1 --interface-name **my-if** --peer-ip-address **my-link-local-IP** --peer-asn **my-ASN** --region **my-region** 

### Configuration - Fortinet FortiGate 300C: CLI

#### Interface Configuration

Configure the Tunnel Interface

```
config system interface
edit "GCP"
    set vdom "root"
    set ip 169.254.0.2 255.255.255
    set type tunnel
    set remote-ip 169.254.0.1
    set snmp-index 15
    set interface "port1"
next
End
```

### **IPsec Configuration**

#### Create the Phase 1 Configuration

```
config vpn ipsec phase1-interface
   edit "GCP"
       set interface "port1"
       set ike-version 2
       set nattraversal disable
       set keylife 36000
       set proposal aes256-shal
        set comments "VPN: GCP (Created by VPN wizard)"
       set dhqrp 15
       set remote-gw 146.148.68.246
       set psksecret ENC
wDfCX7ikIVbjhh9+DAaX0rCO8x/gnuaFu/y1/flQKuh0SLUURBbG7ITM7MQ+y6TG3ZzUxNWIRlruDPZ1gNcqCi/VEEk5S/
vx0DHI81UCBkNz0i1JK7rRdlCQoMepvw+hSU79BlfIPAI2oi7xt+6a6uGYPB3Eszweeqw/YCYQtfyE+fPGl1NQYcMbkXpa
5tBeN6VTLg==
   next
end
```

#### Create the Phase 2 Configuration

```
config vpn ipsec phase2-interface
edit "Lab_2"
set phase1name "GCP"
set proposal aes256-sha1
set dhgrp 15
set replay enable
set keylifeseconds 10800
next
end
```

#### Configure BGP Routing

```
config router bgp
   set as 65501
   set router-id 169.254.0.2
       config neighbor
           edit "169.254.0.1"
               set remote-as 65500
              set send-community6 disable
           next
       end
       config redistribute "connected"
          set status enable
       end
       config redistribute "rip"
       end
       config redistribute "ospf"
       end
       config redistribute "static"
           set status enable
       end
       config redistribute "isis"
       end
       config redistribute6 "connected"
       end
       config redistribute6 "rip"
       end
       config redistribute6 "ospf"
       end
       config redistribute6 "static"
       end
       config redistribute6 "isis"
       end
```

## Configuration - Fortinet FortiGate 300C: GUI

**IPsec Configuration** 

Login to the Fortinet device using a web browser:



From the VPN configuration option, choose Tunnels to set up a new VPN connection and select "Custom VPN Tunnel (No Template)" from the wizard:

FORTINET FortiGate	300C	210 Wizard	Video	() Help	Logout
System	VPN Creation Wizard				
Router					
Policy & Objects	VPW Setup				
Security Profiles	Name				
VPN	Template				
🕀 📲 IPsec	Bialup - FortiClient (Windows, Mac OS, Android)				
Tunnels     Wizard	Site to Site - FortiGate				
Router   Policy & Objects   Security Profiles   VPN   Immass   Vizard   Immass   Vizard   Immass   Immass  <					
B SSL	Dialup - Android (Native L2TP/IPsec)				
	Dialup - Cisco Firewall				
	Site to Site - Cisco				
	Custom VPN Tunnel (No Template)				
	<buck nixt=""> Cancel</buck>				
User & Device					
WiFi Controller					
Log & Report					

Populate the VPN Tunnel configuration **Network** section as pictured below:

Remote Gateway: select "Static IP Address"

**IP Address**: enter the IP address of the Google Cloud VPN Gateway **Interface**: select the **public** interface of the Fortinet device

Dead Peer Detection: select this checkbox to enable DPD

ystem		Edit VPN Tunnel			
outer					
olicy & Objects	Name	GCP			
ecurity Profiles	Comments	VFN. GCP (Cleated by VFN wizard)			
PN	Network		<ul> <li>×</li> </ul>		
BE IPsec	IP Version	IPv4			
Tunnels	Remote Gateway	Static IP Address	•		
- Wizard	IP Address	IP Address 146.148.68.246			
Tunnel Templates	Interface port1 (outside)		•		
B Monitor	Mode Config				
	NAT Traversal				
	Dead Peer Detection				
	IKE Version : 2 Phase 1 Proposal		/ Edit		
	Algorithms : AES2 Diffie-Hellman Gr	56-SHA1 oup : 15			
	Phase 2 Selectors				
	Name Lab_2	Local Address         Remote Address           0.0.0.0/0.0.0.0         0.0.0.0/0.0.0.0	O Add		
		OK Cancel			
er & Device					
iFi Controller					

Populate the VPN Tunnel configuration **Authentication** section as pictured below:

**Method**: for the authentication method select "Pre-Shared Key" **Pre-Shared-Key**: enter the pre-shared key you have chosen to use **IKE**: select IKE version 2

	e 300C				Wizard	Video	(?) Help	Logout
System			Edit VPN Tunnel					
Router Policy & Objects Security Profiles	Name Comments	GCP VPN: GCP (Created	oy VPN wizard)					
VPN	Network Remote Gatewa	y : Static IP Address , In	erface : port1	/ Edit				
• Tunnels • Wizard • Tunnel Templates • 32 SSL & Monitor	Authentication Method Pre-shared Key IKE Version	Pre-shared Ke	×	××				
	Phase 1 Proposa Algorithms : AES Diffie-Hellman (	l 5256-SHA1 Group : 15		/ Edit				
	Phase 2 Selector Name Lab_2	S Local Address 0.0.0.0/0.0.0.0	Remote Address 0.0.0.0/0.0.0.0	© Add				
			OK Cancel					
User & Device								
WiFi Controller								
Log & Report								

Populate the VPN Tunnel configuration **Phase 1 and 2 Proposal** sections as pictured below. Encryption parameters tested for this guide are as follows:

- Diffe-Hellman Group: 15
- Encryption: AES256
- Authentication: SHA1
- Key Lifetime (Phase 1): 36000 seconds
- Key Lifetime (Phase 2): 10800 seconds
- Perfect Forward Secrecy: Enabled

FORTIDET	FortiGate 300C	2 Contraction	Video	(2) Help	Logout
System	Edit VPN Tunnel				
Router Policy & Objects Security Profiles	Name GCP Comments VPN: GCP (Created by VPN wizard)				
VPN	Network         Curr           Remote Gateway : Static IP Address , Interface : port1         Curr				
• Tunnels • Wizard • Tunnel Templates • * SSL • • • Monitor	Authentication / Edit Authentication Method : Pre-shared Key IKE Version : 2				
	Phase 1 Proposal Authentication SHA1 V				
	Diffie-Hellman Group         21         20         19         18         17         16           Key Lifetime (seconds)         36000         36000         36000         36000         36000				
	Name     Local Address     Remote Address     Add       Lab_2     0.0.0.0/0.0.00     0.0.0.0/0.0.00     Image: Constraint of the second seco				
	OK Cancel				
User & Device					
WiFi Controller					
Log & Report					

Populate the VPN Tunnel configuration **Phase 2 Proposal** section as pictured below. Note that for the BGP configuration, only one traffic selector needs to be configured with both **Local Address** and **Remote Address** set to 0.0.0/0.0.0.0. BGP will handle route distribution for any subnets on either side of the tunnel defined by the BGP policy:

FCIRTINET FortiGat	e 300C				15 M O E
System Neuter Pulley & Objects Security Profiles Vern	Algorithms : AUS2 Office Hallman Gr Phane 2 Selectors Name Lu Lub_2 0	10-5HA1 HKP : 15 Scal Address 8.0.0(0.0.0)	Renote Address 8.0.0.075.0.0.0	0AG	
	Edit Phone 2 Name Communits Local Address Remote Address * Advesced	tali,0	•	/×	
	Phase 2 Proposal Encryption AESP Enable Replay Encode Enable Perfect Provent Differentiemen Group Local Pert	Authenticatio n H 1 Secrecy (PIS) H 1 U 21 U H 13 U At H	0AM 0AM 10 10 10 18 17 10 14 14 5 0 2 0 1		
Utore & Orecle #	Pensite Purt Protocol Autolea Koep Alive Acto-regeliate Kar Liteliae Seconds	All of All of D Seconds Moto			
Will I Controller				OK Cancel	

The completed tunnel configuration will appear as shown below:

F	FortiGate 300C					Wizard	Video	(?) Help	Logout
System			Edit VPN	Tunnel				44. 	
Router Policy & Objects Security Profiles	Name Comments	GCP VPN: GCP (Create	d by VPN wizard)						
VPN	Network Remote Gatew	way : Static IP Address , 1	nterface : port1		/ Edit				
Wizard     Wizard     Tunnel Templat     @ @ SSL     @ ■ ■ Monitor	s Authentication IKE Version : :	Authentication / Edit Authentication Method : Pre-shared Key IKE Version : 2							
	Phase 1 Propos Algorithms : A Diffie-Hellmar	Phase 1 Proposal        ZEdit       Algorithms : AE5256-SHA1        Diffie-Hellman Group : 15							
	Phase 2 Selecto Name Lab_2	Local Address	<b>Remote</b> 0.0.0.0	Address /0.0.0.0	O Add				
			ок	Cancel					
User & Device									
WiFi Controller									
Log & Report									

### **Tunnel Interface**

The VPN Wizard used in the <u>IPsec Configuration</u> section will automatically create a virtual tunnel interface which will be used as the IPsec tunnel endpoint. This interface will not have an IP address, however, and the Wizard will not prompt for one. For the BGP configuration, the virtual tunnel inside must be addressed as the BGP peer. Multi-hop BGP is not supported. To add an IP address to the tunnel interface, select **Network** and **Interface** from the sidebar menu. Locate the VPN tunnel entry created by the VPN Wizard and click **Edit**:

FCBRTINET	FortiG	ate 300C					1 Wizard	Video	? Help	Logout
System		FortiGate 3000		7 9 8 10				Group	by Type (	
Interfaces		T Statu	IS V Name	Members	▼ IP/Netmask	⊤ Type	T Access	s V Re		
- • WAN Link Load B	alancing	Physical (1	1)							
- • DNS		<b>P O</b>	port1 (outsi	de)	209.119.81.228 255.255.255.248	🖳 Physical	PING AUTO-IPSEC			3
Packet Capture		O	GCP		0.0.0.0 0.0.0.0	VPN Tunnel			( <u></u> )	6
Config		0	port2 (inside	=)	192.168.2.4 255.255.255.0	Physical	PING HTTPS SSH HTTP FMC	3-Access		4
SNMP		0	port3		0.0.0.0 0.0.0.0	Physical				0
- Replacement Mes	ssages	0	port4		10.10.10.1 255.255.255.0	Physical	PING FMG-Access			0
- • FortiGuard		0	ports		0.0.0 0.0.0.0	Physical				0
- • FortiSandbox		0	port6		0.0.0.0.0.0.0	Physical				0
- • Advanced		, in the second se	port/		0.0.0.0.0.0.0	Physical				0
Features		ő	porta		0.0.0.0.0.0.0	Physical Rhysical				0
Admin		0	port10		0.0.0.0.0.0.0.0	Physical				0
B 💭 Monitor										
Router										
Policy & Objects										
Security Profiles										
VPN										
User & Device										
WiFi Controller										
Log & Report										

The **Edit Interface** UI allows the **IP** and **Remote IP** for the tunnel interface to be set. The IP should be set to the BGP peer address allocated to the remote location in the <u>Google Cloud</u> <u>Router VPN Tunnel configuration</u> section and the Remote IP should be set to the address allocated to the Google Cloud Router. After entering the appropriate IP info, click **OK**:

FCRTINET FortiG	ate 300C		2:0 Wizard	Video	() Help	Logout
System		Edit Interface				
Oashboard     Status     Status     Status     Interfaces     WAN Link Load Balancing     DNS     Packet Capture     Config     Replacement Messages     FortiGuard     FortiGard     FortiGard     FortiGard     FortiGard     Sources     Config     C	Interface Name Type Interface Addressing mode IP Remote IP Administrative Access DHCP Server Security Mode Listen for RADIUS Accounting Messages Comments Administrative Status	GCP Tunnel Interface port1 Manual 169.254.0.2 169.254.0.1 HTTPS PING HTTP FMG-Access CAPWA SSH SNMP FCT-Access Enable None V OK Cancel	P			
Router Policy & Objects Security Profiles VPN User & Device WiFi Controller Log & Report						

#### The VPN Tunnel interface should display the configured IP address:

FORTINET Fortig	Sate	300C						Wizard Video	Pelp Logou
System S Dashboard - Status B M FortiView	Fort	SATINET	r.		9	<b></b>			
🖻 🚊 Network	0	Create Ne	w 🕶	📝 Edit 📲	Delete			Group	by Type 🔵
Interfaces		▼ Status	5	7 Name	▼ Members	▼ IP/Netmask	🔻 Type	\ Access	🔻 Ref. 🕻
- • WAN Link Load Balancing	Phy	ysical (11	)						
- • DNS	P	0	port1	(outside)		209.119.81.228 255.255.255.248	Physical	PING AUTO-IPSEC	3
Packet Capture	Inte	0	GCP			169.254.0.2 255.255.255.255	(•) VPN Tunnel		4
Admin		0	port2	(inside)		192.168.2.4 255.255.255.0	Physical	PING HTTPS SSH HTTP FMG-Access	4
Certificates		0	ports			10 10 10 1 255 255 255 0	Physical     Dhusiaal	DING FMC Assess	0
Monitor		0	port4			0.0.0.0.0.0.0	Physical	PING PMG-Access	0
		0	north				Physical		0
		0	port7			0.0.0.0 0.0.0.0	Physical		0
		0	port8			0.0.0.0 0.0.0.0	Physical		0
	1	0	port9			0.0.0.0 0.0.0.0	Physical		0
	-	0	port1	0		0.0.0.0 0.0.0.0	🔄 Physical		0
			porta	-					
Router									
Policy & Objects									
ecurity Profiles									
PN									
ser & Device									
iFi Controller									

### BGP

The final step is to configure BGP routing. From the **Routing** section in the sidebar menu, select **Dynamic**, then **BGP**. Local and neighbor BGP info must be entered to complete the BGP configuration. BGP parameters set in the <u>Google Cloud Router configuration section</u> are used here:

- Local AS: the Autonomous System number set for the remote peer
- Router ID: the IP address set for the remote peer
- Neighbor IP: the IP address set for the Google Cloud Router
- **Remote AS**: the Autonomous System number set for the **Google Cloud Router**

FCRTINET	FortiGate 300	С				1 3 Wizard	Video	<b>?</b> Help	Logout
System Router	Local Route	As  65501 r ID 169.254.0.2	(1-4294967295) (IP) <b>App</b>	ly					
<ul> <li>Static Routes</li> <li>Policy Routes</li> </ul>	Neighbo	ors		IP:	Remote As:		Ado	l / Edit	
Settings	🗂 Delete								
E Y Dynamic		Neighbor		Remote	As				
• OSPF		169.254.0.1		65500					
= BGP	Networ	ks		IP/Netmask				Add	
Multicast	🛅 Delete								
a 🚽 Monitor		Network							
				No BGP network defined.					
Policy & Objects									
Security Profiles									
VPN									
User & Device									
WiFi Controller									
Log & Report									

## Testing the Site-to-Site VPN

## Verify Connectivity

To verify that Cloud Router has successfully initiated BGP peering with AWS, check the Cloud Router status in the Developer Console:

	Google Cloud Platform				٩				
~	Networking	Cloud Routers	+ CRE	ATE ROUTER	T DELET	ΓE			
8	Networks	Name A	Network	Region	Google ASN	VPN Gateway	VPN tunnels	BGP sessions	Logs
c	External IP addresses	gcp-to-fg300c-router	to-fg300c	us-central1	65500	gcp-to-fortinet-fg300c	gcp-to-fortinet-fg300c-tunnel-1	gcp-to-fortinet-fg300c-bgp	View
35	Firewall rules								
>\$	Routes								
A	Load balancing								
里	Cloud DNS								
- 52	VPN								
***	Cloud Routers								

To verify that the IPsec tunnel has been successfully initiated, check the VPN status in the Developer Console:

≡	Google Cloud Platform					٩					
₹.	Networking		ATE VPN CON	INECTION	DELETE						
82	Networks	Name	Network	Region	IP address	Remote peer IP address	Ø	Cloud routers	Log	Firewall rules 👩	
면	External IP addresses	gcp-to-fortinet-fg300c	to-lab	us-central1	146.148.68.246 🔞	209.119.81.228		gcp-to-fg300c-router	View	Configure	
88	Firewall rules										
×	Routes										
A	Load balancing										
9	Cloud DNS										
- 52	VPN										
***	Cloud Routers										

## Testing the Tunnel

#### **Basic Ping**

To test the IPsec tunnel traffic selectors, ping a host on each subnet specified in the tunnel configuration from a host attached to the Google Cloud Platform network:

