

# Skillet for PAN-OS

---



## GCP VPN Gateway

## IKE/IPSec and BGP configuration for PAN-OS

<https://github.com/cestebanez91/GCP-VPN-PANOS>

## Table of Contents

---

1.	<b>Presentation of the Skillet .....</b>	<b>3</b>
2.	<b>Diagram .....</b>	<b>4</b>
3.	<b>Run Skillet .....</b>	<b>5</b>

# **1. Presentation of the Skillet**

This skillet will configure IKE/IPSec parameters and BGP in order to connect PAN-OS to GCP VPN Gateway.

This skillet will be used to connect your Palo Alto Network device (physical or VM-series) to any GCP VPN IPSec Gateway to establish a secure VPN connection.

By default, GCP propose two IPSec tunnels for each configured connection, this skillet will configure both tunnels.

Based on parameters given by GCP once you configured:

- GCP Cloud VPN Gateway with interface:0 and interface:1.
- GCP Peer VPN Gateway setup.
- GCP Cloud VPN Tunnel.

It will create two new IKE gateways and two new Ipsec tunnels, whatever these are already existing, iteration is possible up to four IKE gateways and four IPSec tunnels.

IKE and IPSec profile are compliant to GCP VPN crypto profiles expectations.

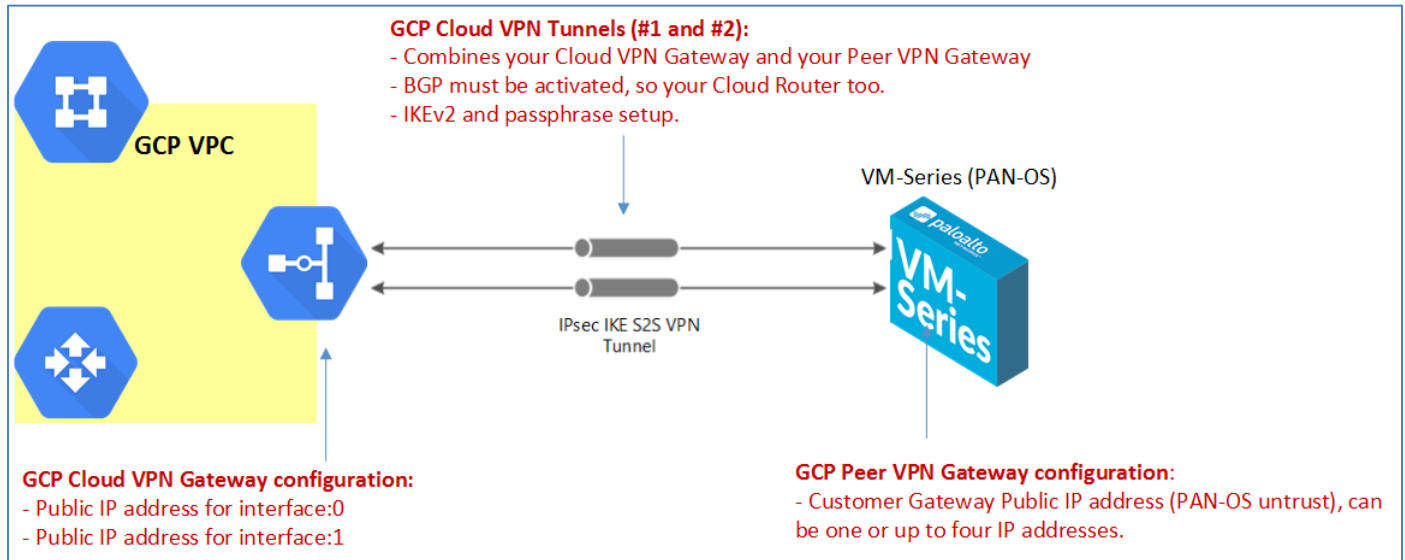
**This skillet will configure PAN-OS with following features:**

- IKE crypto profile compliant with GCP VPN
- IPSec crypto profile compliant with GCP VPN
- IKE gateway to connect to GCP Cloud VPN Gateway interface:0
- IKE gateway to connect to GCP Cloud VPN Gateway interface:1
- IPSec tunnel 1 and 2
- Tunnel interfaces, and Zone « VPN »
- Routing and BGP configuration with distribution profile activated for connected routes

**Content is the following:**

- ikecrypto.xml will configure IKE crypto profile
- ipseccrypto.xml will configure IPSec crypto profile
- ikeprofile.xml will configure IKE gateways with iteration
- ipsecprofile.xml will configure IPSec tunnels with iteration
- interface.xml will configure tunnels
- zone.xml will configure zones
- routing.xml will configure BGP parameters to exchange routes

## 2. Diagram



With GCP, the Peer VPN Gateway can have from one to four interfaces, we decided to use only one interface (one IP public IP address) to establish both tunnel #1 and #2 to GCP Cloud VPN Gateway.

The GCP Cloud VPN Gateway will use two interfaces, so two different public IP addresses.

To establish an IPsec connection to your GCP Cloud VPN Gateway, you will need to configure as a prerequisite:

- **GCP Cloud VPN Gateway deployed and attached to a VPC**
- **GCP Cloud Peer Gateway configured (your on prem device running PAN-OS)**
- **GCP Cloud VPN Tunnels with BGP activated and configured (/30 defined by yourself)**
- **PAN-OS device 7.1 min**

### 3. Run Skillet

When you run exectue the skillet, you need to define these values:

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17

PAN-OS Configuration

Customize PAN-OS Skillet: GCP VPN IKE/IPSec

Give a name to your AWS VPN configuration:

GoogleVPN

Public IP address of your PAN-OS device to connect to GCP VPN Gateway for both tunnels:

168.61.145.99

Public IP address of GCP VPN Gateway for tunnel 1, Interface 0:

35.242.79.226

Public IP address of GCP VPN Gateway for tunnel 2, Interface 1:

35.220.123.115

GCP BGP Peer for tunnel 1:

169.254.1.1

GCP BGP Peer for tunnel 2:

169.254.2.1

GCP VGW BGP AS - Specify your GCP BGP AS if custom. Must match the value you configure in GCP VPN gateway BGP configuration.

65500

PAN-OS ethernet interface for IKE/IPsec - Ethernet interface for untrust initiating the VPN connection:

ethernet1/1

PAN-OS Tunnel 1 interface number - If you are using an existing tunnel interface, opt for another than tunnel.1:

tunnel.1

IP address for tunnel 1 interface (same as BGP Peer ID defined in GCP for remote device, must be with /30):

169.254.1.2/30

PAN-OS IKE preshared key for tunnel 1:

paloalto

PAN-OS Tunnel 2 interface number - If you are using an existing tunnel interface, opt for another than tunnel.2:

tunnel.2

IP address for tunnel 2 interface (same as BGP Peer ID defined in GCP for remote device, must be with /30):

169.254.2.2/30

PAN-OS IKE preshared key for tunnel 2:

paloalto

PAN-OS virtual router name - If you want to use another than default virtual router instance.

default

PAN-OS BGP Router ID (same as BGP Peer ID defined in GCP for remote device, without /30):

169.254.1.2

PAN-OS BGP AS - Specify your local BGP AS if needed. Must match the value you configure in AWS Customer Gateway.

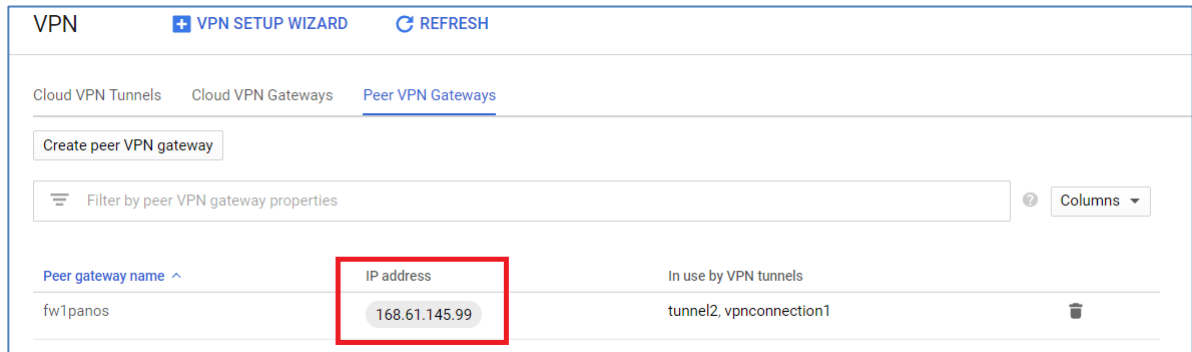
65000

Submit

## Palo Alto Networks – Skillet GCP VPN for PAN-OS

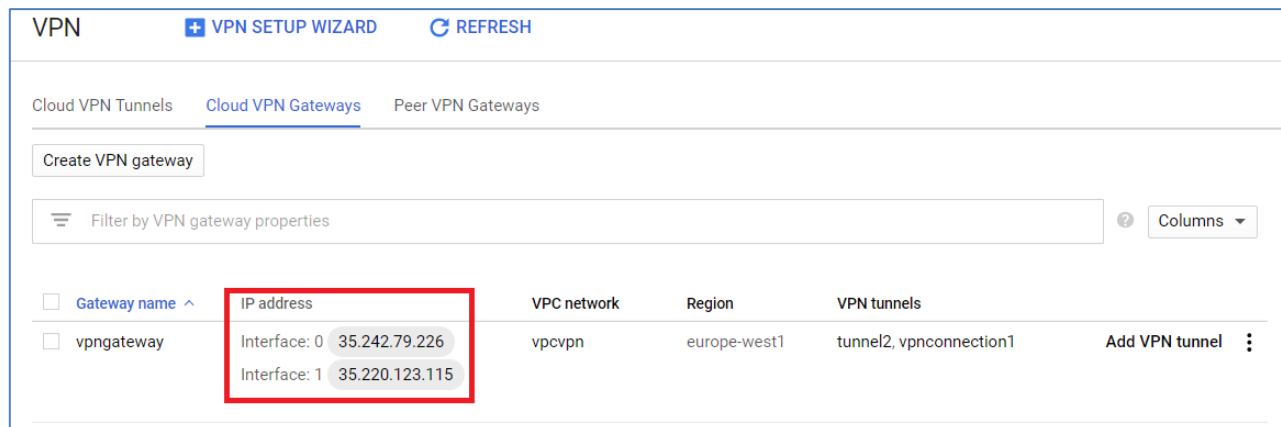
**1:** Give a name to your VPN connection, this name will prename all IKE and IPsec parameters to distinguish this VPN connection.

**2:** This is the public IP address of your PAN-OS device (GCP Cloud Peer Gateway), we need it as this is a parameter used for IKEv2 peer identification in IKE profiles. This is the value shown below:



VPN			
<a href="#">+ VPN SETUP WIZARD</a> <a href="#">REFRESH</a>			
Cloud VPN Tunnels   Cloud VPN Gateways <u>Peer VPN Gateways</u>			
<a href="#">Create peer VPN gateway</a>			
<input type="text" value="Filter by peer VPN gateway properties"/> <a href="#">Columns</a>			
Peer gateway name ^	IP address	In use by VPN tunnels	
fw1panos	168.61.145.99	tunnel2, vpnconnection1	

**3 and 4:** These are the GCP Cloud VPN Gateway IP addresses for interface:0 and interface:1, as shown below:



VPN					
<a href="#">+ VPN SETUP WIZARD</a> <a href="#">REFRESH</a>					
Cloud VPN Tunnels <u>Cloud VPN Gateways</u> Peer VPN Gateways					
<a href="#">Create VPN gateway</a>					
<input type="text" value="Filter by VPN gateway properties"/> <a href="#">Columns</a>					
<input type="checkbox"/> Gateway name ^	IP address	VPC network	Region	VPN tunnels	
<input type="checkbox"/> vpngateway	Interface: 0 35.242.79.226 Interface: 1 35.220.123.115	vpcvpn	europa-west1	tunnel2, vpnconnection1	<a href="#">Add VPN tunnel</a>

**5 and 6:** These are GCP Cloud VPN Tunnels BGP Peer IDs for tunnel 1 and tunnel 2, as shown below:

VPN <span>VPN SETUP WIZARD</span> <span>REFRESH</span> <span>DELETE</span>						
<a href="#">Cloud VPN Tunnels</a> <a href="#">Cloud VPN Gateways</a> <a href="#">Peer VPN Gateways</a>						
<a href="#">Create VPN tunnel</a>						
Filter by VPN tunnel properties						
<input type="checkbox"/> Tunnel name	Cloud VPN gateway (IP) ^	Peer VPN gateway (IP)	Cloud Router BGP IP	BGP Peer IP	Routing type	
<input type="checkbox"/> tunnel2	vpngateway 35.220.123.115	fw1panos 168.61.145.99	169.254.2.1	169.254.2.2	Dynamic (BGP)	
<input type="checkbox"/> vpnconnection1	vpngateway 35.242.79.226	fw1panos 168.61.145.99	169.254.1.1	169.254.1.2	Dynamic (BGP)	

**7:** You need to define the GCP Cloud VPN Tunnel BGP AS number, this value can be found in the detail of your Tunnel configuration in GCP console:

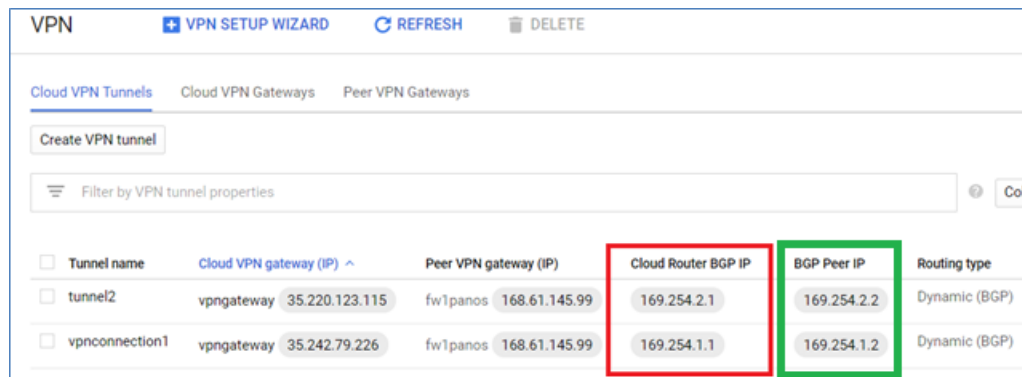
VPN tunnel details <span>DELETE</span>	
<b>tunnel2</b> Status: No incoming packets from peer	
<a href="#">Details</a> <a href="#">Monitoring</a>	
Remote peer gateway	
Name	fw1panos
IP address	168.61.145.99
Cloud VPN gateway	
Name	vpngateway (High-availability gateway)
VPC network	vpcvpn
Region	europa-west1
IP address	Interface: 1 35.220.123.115
Logs	<a href="#">View</a>
Routing and security	
Routing type	Dynamic (BGP)
Cloud router	virtualrouter
Cloud router ASN	65500
Peer router ASN	65000
BGP session	bgptunnel2 (⚠️ Waiting for peer ) <a href="#">Modify BGP session</a>
Cloud Router BGP IP address	169.254.2.1
BGP peer IP address	169.254.2.2
IKE version	IKEv2

## Palo Alto Networks – Skillet GCP VPN for PAN-OS

**8:** Choose from ethernet1/1 to ethernet1/4 on which PAN-OS interface your IKE gateway will terminate (commonly untrust interface is ethernet1/1)

**9:** For Tunnel #1, choose from tunnel.1 to tunnel.4 to create the new PAN-OS tunnel interface if tunnels are already existing.

**10:** Give an IP address to your Tunnel #1 tunnel interface, this value has to be /30 and must match your BGP configuration in GCP as below in green:



<input type="checkbox"/>	Tunnel name	Cloud VPN gateway (IP)	Peer VPN gateway (IP)	Cloud Router BGP IP	BGP Peer IP	Routing type
<input type="checkbox"/>	tunnel2	vpngateway 35.220.123.115	fw1panos 168.61.145.99	169.254.2.1	169.254.2.2	Dynamic (BGP)
<input type="checkbox"/>	vpnconnection1	vpngateway 35.242.79.226	fw1panos 168.61.145.99	169.254.1.1	169.254.1.2	Dynamic (BGP)

**11:** Preshared key for Tunnel #1 IKE gateway, can be found in section, this is the same as defined when you created your GCP Cloud VPN Gateway passphrase.

**12, 13 and 14:** Same as #Tunnel1 but for #Tunnel 2 informations.

**15:** Type in the name of your PAN-OS virtual router instance to be configured (by default: default).

**16:** Fill with the PAN-OS BGP Peer ID, this value is unique for both tunnels (we use only one unique virtual router instance), this can be found in section and is the same as tunnel1 interface IP address.

**17:** Local BGP AS Number for PAN-OS, by default 65000. This skillet will not update your GCP Cloud Tunnel configuration (Peer Router ASN) if different.