

DrayTek

VPN

Google Cloud Platform

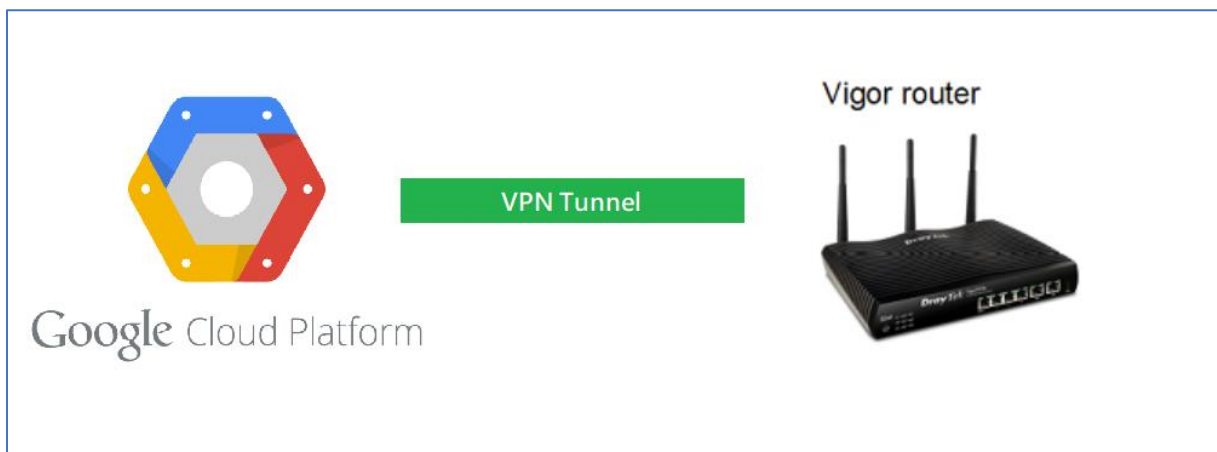


Google Cloud Platform

Google Cloud Platform is een cloud service die door google wordt aangeboden. Op dit platform kunnen gebruikers hun eigen virtuele servers opzetten, bestanden delen en hun data beheren.

Google Cloud Platform ondersteunt IPSec VPN verbinding om de overdracht van gegevens optimaal te beveiligen. Onderstaand de uitleg over hoe u een VPN verbinding tot stand kunt brengen tussen een Vigor router en Google Cloud Platform.

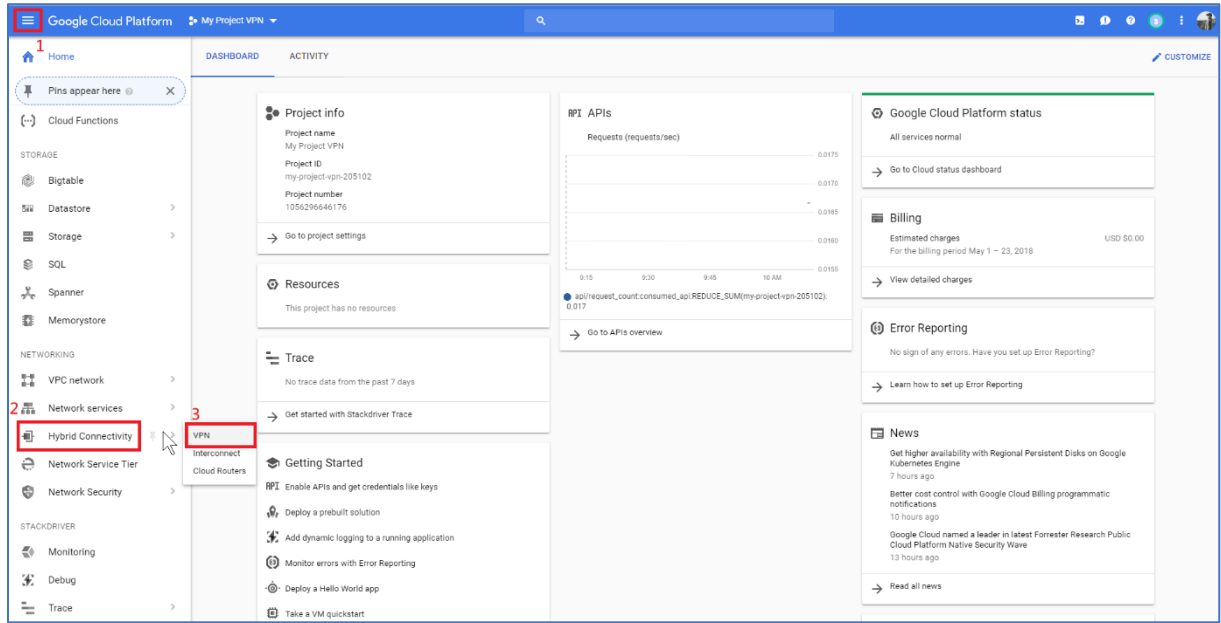
In deze handleiding zullen wij middels enkele stappen uitleggen hoe u een VPN verbinding kunt opzetten tussen de DrayTek en het Google Cloud Platform.



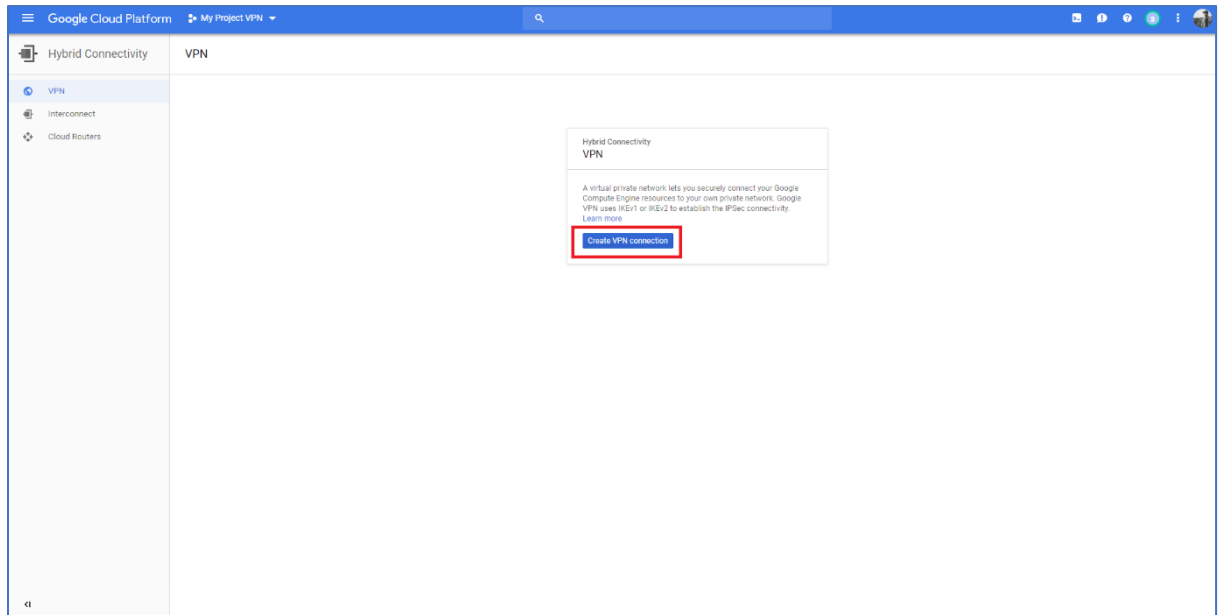
Google Cloud Platform configuratie

1. Open Google Cloud Platform

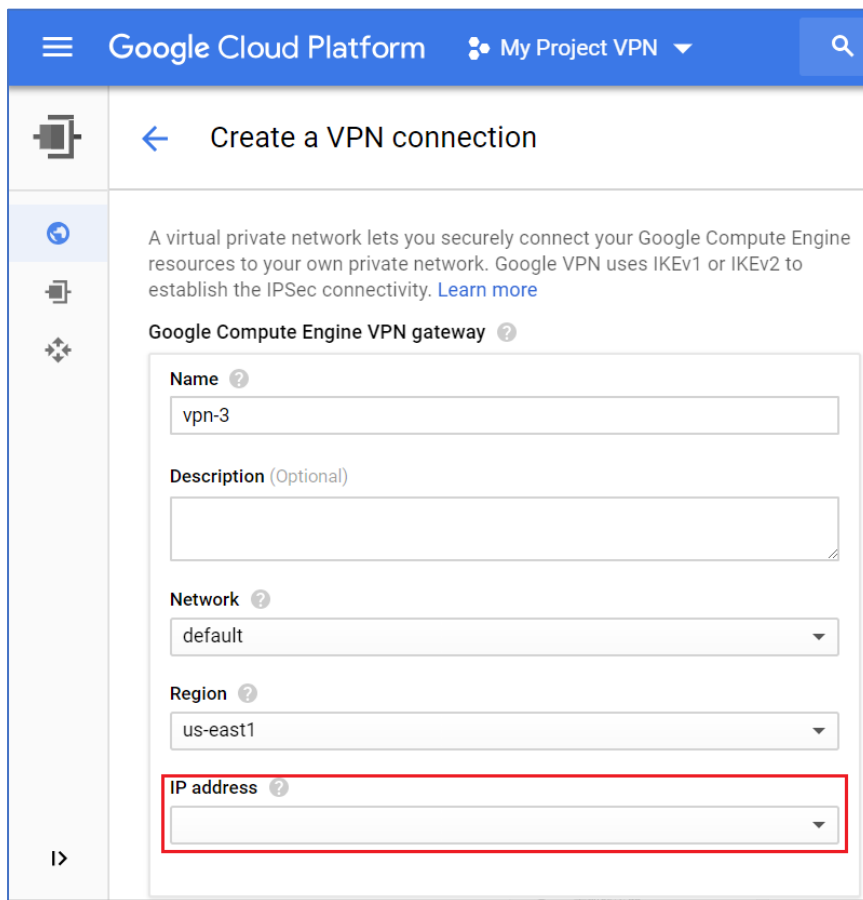
- Klik op **Menu**
- Klik op **Hybrid Connectivity**
- Klik op **VPN**



2. Klik op **Create VPN Connection**

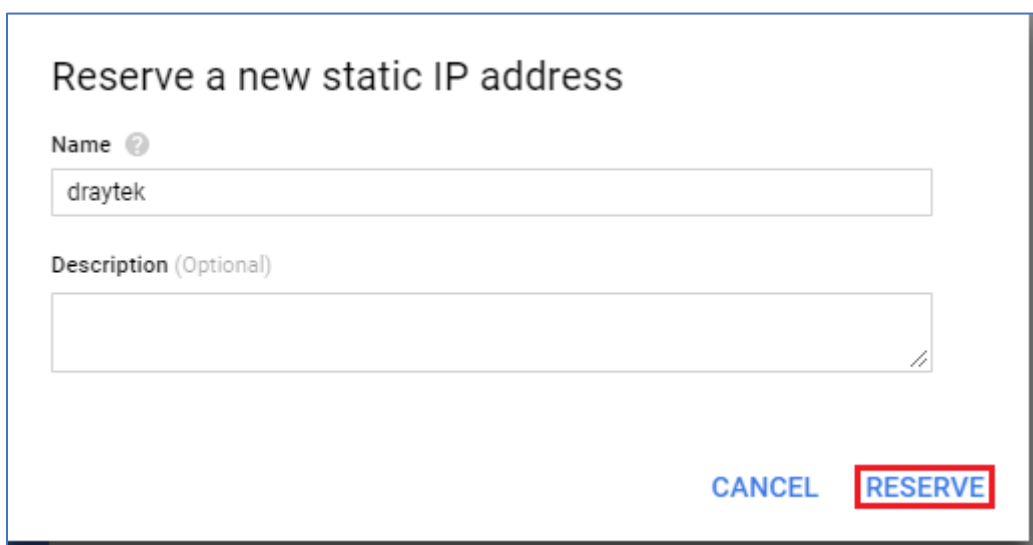


3. Selecteer **Region** en klik op **IP address**



The screenshot shows the Google Cloud Platform console interface for creating a VPN connection. The page title is "Create a VPN connection". Below the title, there is a brief description of a virtual private network and a link to "Learn more". The main form is titled "Google Compute Engine VPN gateway" and contains several fields: "Name" (filled with "vpn-3"), "Description (Optional)" (empty), "Network" (dropdown menu with "default" selected), "Region" (dropdown menu with "us-east1" selected), and "IP address" (dropdown menu, highlighted with a red box). The "IP address" field is currently empty.

4. Nadat u op IP adres heeft geklikt, kunt u een naam invullen. Google geeft een extern IP adres vrij voor de VPN verbinding.



The screenshot shows the "Reserve a new static IP address" form. It has a title "Reserve a new static IP address" and two input fields: "Name" (filled with "draytek") and "Description (Optional)" (empty). At the bottom right, there are two buttons: "CANCEL" and "RESERVE". The "RESERVE" button is highlighted with a red box.

Klik **Reserve** om op te slaan.

5. Tunnel settings:

- Vul het externe (internet) IP adres van uw Vigor router in bij **Remote peer IP address**
- Bij IKE version selecteer **IKEv2**
- Vul de **Shared secret** in
- Selecteer **Route-based** in **Routing options**
- Vul hier uw **Remote network IP ranges** in (subnet van uw Vigor router)

Tunnels ?
You can have multiple tunnels to a single Peer VPN gateway

New item [trash] [close]

Name ?
vpn-2-tunnel-1

Description (Optional)
[text area]

Remote peer IP address ?
Internet IP of your Vigor router

IKE version ?
IKEv2

Shared secret ?
1234

Routing options ?
Dynamic (BGP) **Route-based** Policy-based

Remote network IP ranges ?
Enter multiple IP address ranges (in CIDR notation) by pressing Enter after each one
192.168.1.0/24 [x]

[Done] [Cancel]

[+ Add tunnel]

[Create] [Cancel]

6. Klik op **Network** in de VPN interface

VPN [CREATE]

Google VPN Tunnels Google VPN Gateways

Filter by VPN gateway properties [help] Columns

<input type="checkbox"/> Gateway name ^	Google IP address	Network	Region	Tunnels
<input type="checkbox"/> vpn-1	35.237.209.49	default	us-east1	
<input type="checkbox"/> vpn-1	35.186.185.183	default	us-east4	vpn-2-tunnel-1

- Het netwerk van dit project zal op deze pagina worden getoond.
Het IP-adres van de regio die u in Stap 3 heeft geselecteerd, zal hier ook worden getoond. We zullen later dat adres gaan gebruiken.

default

Description
Default network for the project

Subnet creation mode
Auto subnets

Dynamic routing mode
Regional

Subnets Static internal IP addresses Firewall rules Routes VPC Network Peering

[Add subnet](#) Flow logs ▾

<input type="checkbox"/>	Name ^	Region	IP address ranges	Gateway	Private Google access	Flow logs ?	
<input type="checkbox"/>	default	us-central1	10.128.0.0/20	10.128.0.1	Off	Off	
<input type="checkbox"/>	default	europa-west1	10.132.0.0/20	10.132.0.1	Off	Off	
<input type="checkbox"/>	default	us-west1	10.138.0.0/20	10.138.0.1	Off	Off	
<input type="checkbox"/>	default	asia-east1	10.140.0.0/20	10.140.0.1	Off	Off	
<input type="checkbox"/>	default	us-east1	10.142.0.0/20	10.142.0.1	Off	Off	
<input type="checkbox"/>	default	asia-northeast1	10.146.0.0/20	10.146.0.1	Off	Off	
<input type="checkbox"/>	default	asia-southeast1	10.148.0.0/20	10.148.0.1	Off	Off	
<input type="checkbox"/>	default	us-east4	10.150.0.0/20	10.150.0.1	Off	Off	
<input type="checkbox"/>	default	australia-southeast1	10.152.0.0/20	10.152.0.1	Off	Off	
<input type="checkbox"/>	default	europa-west2	10.154.0.0/20	10.154.0.1	Off	Off	
<input type="checkbox"/>	default	europa-west3	10.156.0.0/20	10.156.0.1	Off	Off	
<input type="checkbox"/>	default	southamerica-east1	10.158.0.0/20	10.158.0.1	Off	Off	
<input type="checkbox"/>	default	asia-south1	10.160.0.0/20	10.160.0.1	Off	Off	
<input type="checkbox"/>	default	northamerica-northeast1	10.162.0.0/20	10.162.0.1	Off	Off	
<input type="checkbox"/>	default	europa-west4	10.164.0.0/20	10.164.0.1	Off	Off	

DrayTek Configuratie

8. Ga naar VPN and Remote Access >> LAN to LAN, en klik op een index nummer.
 - Vul een **profiel naam** in
 - Vink **Enable this profile** aan
 - Selecteer **Dial-in**

VPN and Remote Access >> LAN to LAN

Profile Index : 1

1. Common Settings

Profile Name <input type="text" value="Google"/>	Call Direction <input type="radio"/> Both <input type="radio"/> Dial-Out <input checked="" type="radio"/> Dial-in
<input checked="" type="checkbox"/> Enable this profile	Tunnel Mode <input type="radio"/> GRE Tunnel
VPN Dial-Out Through <input type="text" value="WAN1 First"/>	<input type="checkbox"/> Always on
Netbios Naming Packet <input checked="" type="radio"/> Pass <input type="radio"/> Block	Idle Timeout <input type="text" value="300"/> second(s)
Multicast via VPN <input type="radio"/> Pass <input checked="" type="radio"/> Block <small>(for some IGMP,IP-Camera,DHCP Relay..etc.)</small>	<input type="checkbox"/> Enable PING to keep IPsec tunnel alive
	PING to the IP <input type="text"/>

9. Selecteer **IPSec Tunnel** bij Allowed Dial-In Type
 - Stel volgens **step 6**, het overeenkomstige netwerk IP en subnet mask uit uw regio in bij
Remote network IP en **Remote Network Mask**
 - Voer uw lokale IP-adres en mask in bij **Local Network IP** en **Local Network Mask**

3. Dial-In Settings

Allowed Dial-In Type

<input type="checkbox"/> PPTP	Username <input <="" td="" type="text" value="???"/>
<input checked="" type="checkbox"/> IPsec Tunnel	Password(Max 11 char) <input type="text"/>
<input type="checkbox"/> L2TP with IPsec Policy <input type="text" value="None"/>	VJ Compression <input checked="" type="radio"/> On <input type="radio"/> Off
<input type="checkbox"/> SSL Tunnel	IKE Authentication Method
<input type="checkbox"/> Specify Remote VPN Gateway	<input checked="" type="checkbox"/> Pre-Shared Key
Peer VPN Server IP <input type="text"/>	<input type="text" value="IKE Pre-Shared Key"/>
or Peer ID <input type="text"/>	<input type="checkbox"/> Digital Signature(X.509)
	<input type="text" value="None"/>
	Local ID
	<input checked="" type="radio"/> Alternative Subject Name First
	<input type="radio"/> Subject Name First
	IPsec Security Method
	<input checked="" type="checkbox"/> Medium(AH)
	High(ESP) <input checked="" type="checkbox"/> DES <input checked="" type="checkbox"/> 3DES <input checked="" type="checkbox"/> AES

4. GRE Settings

Enable IPsec Dial-Out function GRE over IPsec

Logical Traffic My GRE IP Peer GRE IP

5. TCP/IP Network Settings

My WAN IP <input type="text" value="0.0.0.0"/>	RIP Direction <input type="text" value="Disable"/>
Remote Gateway IP <input type="text" value="0.0.0.0"/>	From first subnet to remote network, you have to do <input type="text" value="Route"/>
Remote Network IP <input type="text" value="10.158.0.0"/>	<input type="checkbox"/> IPsec VPN with the Same Subnets
Remote Network Mask <input type="text" value="255.255.240.0"/>	<input type="checkbox"/> Change default route to this VPN tunnel (Only active if one single WAN is up)
Local Network IP <input type="text" value="192.168.1.1"/>	
Local Network Mask <input type="text" value="255.255.255.0"/>	
<input type="button" value="More"/>	

10. Ga naar **VPN and Remote Acces >> IPsec General Setup**, Vul een **Pre-Shared Key** in, Deze key moet overeenkomen met de Shared secret in **stap 5**. Bevestig de key en klik op OK.

VPN and Remote Access >> IPsec General Setup

VPN IKE/IPsec General Setup
Dial-in Set up for Remote Dial-in users and Dynamic IP Client (LAN to LAN).

IKE Authentication Method
Certificate for Dial-in: None ▾
Pre-Shared Key
Pre-Shared Key: [masked]
Confirm Pre-Shared Key: [masked]

IPsec Security Method
 Medium (AH)
Data will be authentic, but will not be encrypted.

High (ESP) DES 3DES AES
Data will be encrypted and authentic.

OK Cancel

11. Wanneer de configuratie aan beide kanten juist is zal de VPN verbinding online komen. Bij VPN and Remote Access >> Connection Management kunt u de status van de VPN verbinding terugvinden.

VPN and Remote Access >> Connection Management

Dial-out Tool
General Mode: [dropdown] Dial
Backup Mode: [dropdown] Dial
Load Balance Mode: [dropdown] Dial

VPN Connection Status

LAN-to-LAN VPN Status			Remote Dial-in User Status					
VPN	Type	Remote IP	Virtual Network	Tx Pkts	Tx Rate(bps)	Rx Pkts	Rx Rate(bps)	UpTime
1 (Google)	IKEv2 IPsec Tunnel AES-SHA1 Auth	35.192.146.191 via WAN2	10.158.0.0/20	0	0	0	0	0:1:17

xxxxxxx : Data is encrypted.
xxxxxxx : Data isn't encrypted.

VPN CREATE DELETE

Google VPN Tunnels Google VPN Gateways

Filter by VPN tunnel properties Columns

Tunnel name	Status	Google gateway	Google IP address	Google network	Region	Peer IP address	Routing type
vpn-2-tunnel-1	Established	vpn-2	35.192.146.191	default	us-central1	118.166.185.250	Route-based

Voorbehoud

We behouden ons het recht voor om deze en andere documentatie te wijzigen zonder de verplichting gebruikers hiervan op de hoogte te stellen. Afbeeldingen en screenshots kunnen afwijken.

Copyright verklaring

© 2020 DrayTek

Alle rechten voorbehouden. Niets uit deze uitgave mag worden verveelvoudigd, opgeslagen in een geautomatiseerd gegevensbestand en/of openbaar gemaakt in enige vorm of op enige wijze, hetzij elektronisch, mechanisch, door fotokopieën, opnamen of op enige andere manier zonder voorafgaande schriftelijke toestemming van de uitgever.

Ondanks alle aan de samenstelling van deze handleiding bestede zorg kan noch de fabrikant, noch de auteur, noch de distributeur aansprakelijkheid aanvaarden voor schade die het gevolg is van enige fout uit deze uitgave.

Trademarks

Alle merken en geregistreerde merken zijn eigendom van hun respectievelijke eigenaren.