Google Cloud VPN Interop Guide

Using Cloud VPN with A Palo Alto Networks® Firewall

Model: PA-3020

Contents

Introduction

This guide walks you through the process of configuring the Palo Alto Networks PAN-3020 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.

All IP Addresses are example only

Environment overview

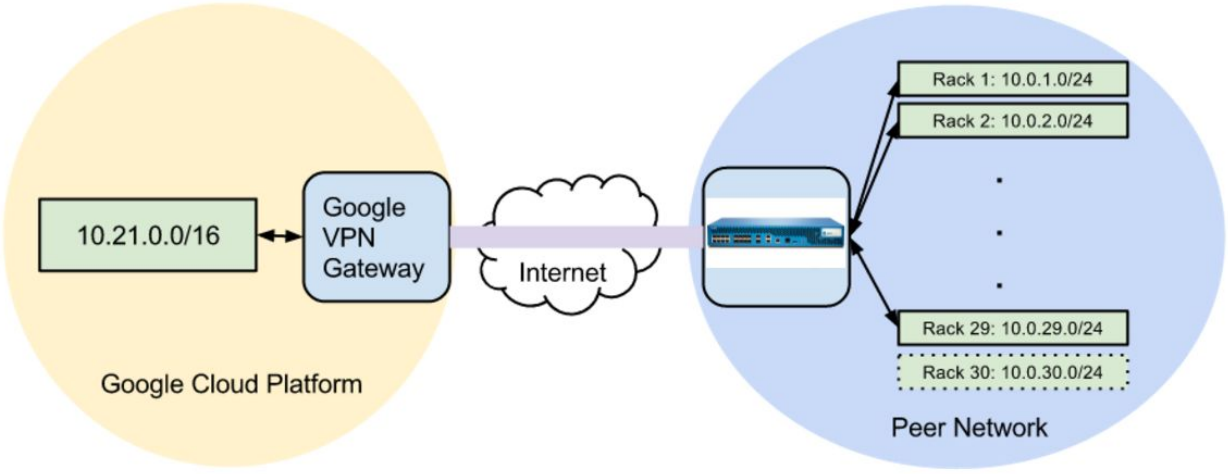
The equipment used in the creation of this guide is as follows:

Vendor:	Palo Alto Networks
Model:	PA-3020
Software Revision:	8.1.0

Topology

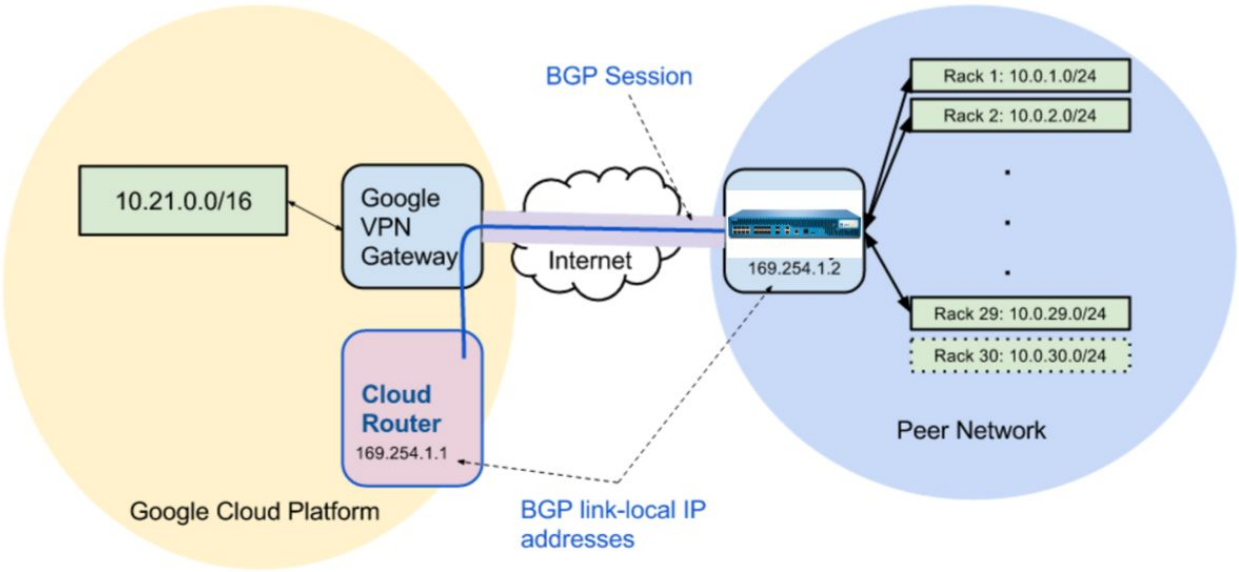
This guide describes two Cloud VPN connection topologies:

1. A site-to-site policy based IPsec VPN tunnel configuration using static routing.



IP Addresses for illustrative purposes only

2. A site-to-site IPsec VPN tunnel configuration using the Google Cloud Router and BGP, also known as *dynamic routing*.



IP Addresses for illustrative purposes only

Configuration

Overview

The configuration samples that follow include numerous value substitutions provided as examples only. When following this guide, replace any references to IP addresses, device IDs, shared secrets or keys, account information, or project names with the appropriate values for your environment. Values unique to your environment are highlighted in **bold**.

This guide is not meant to be a comprehensive overview of the setup for the referenced device, but 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:

1. Selecting the appropriate IPsec configuration
2. Configuring the internet facing interface of your device (outside interface)
3. Configuring Internet Key Exchange (IKE) and IPSec
4. Testing the tunnel

Getting started

The first step in configuring your Palo Alto Networks PA-3020 for use with the Google Cloud VPN service is to ensure that your device meets the following prerequisite conditions:

- Your Palo Alto Networks PA-3020 is online and functional with no faults detected
- You have root access to the Palo Alto Networks PA-3020
- There is at least one configured and verified functional internal interface
- There is one configured and verified functional external interface

IPsec parameters

Use the following values for the IPSec configuration of your PAN-3020.

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

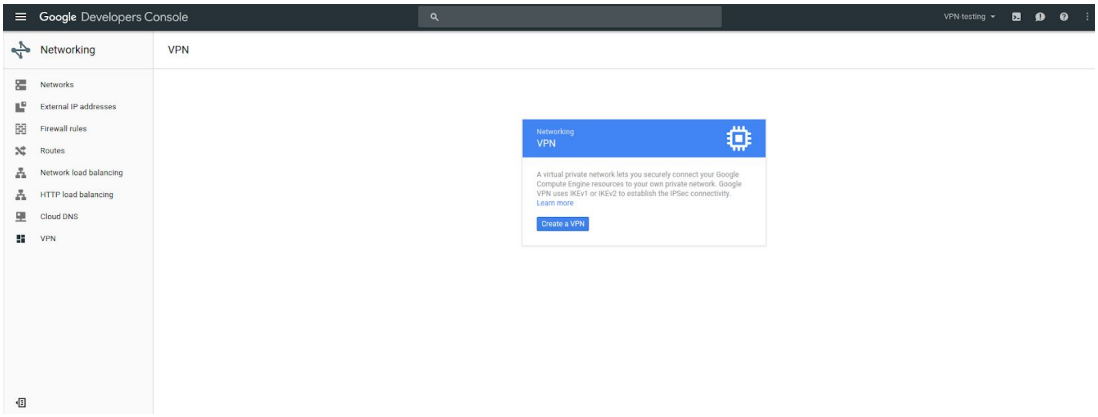
This guide uses the following IKE ciphers.

Phase	*Cipher Role*	*Cipher*
Phase 1	*Encryption*	*aes-256*
	Integrity	*sha-256*
	prf	*sha1-96*
	Diffie-Hellman (DH)	*Group 14*
	Phase 1 lifetime	*36,000 seconds (10 hours)*
Phase 2	*Encryption*	*aes-cbc-256*
	Integrity	*sha-256*

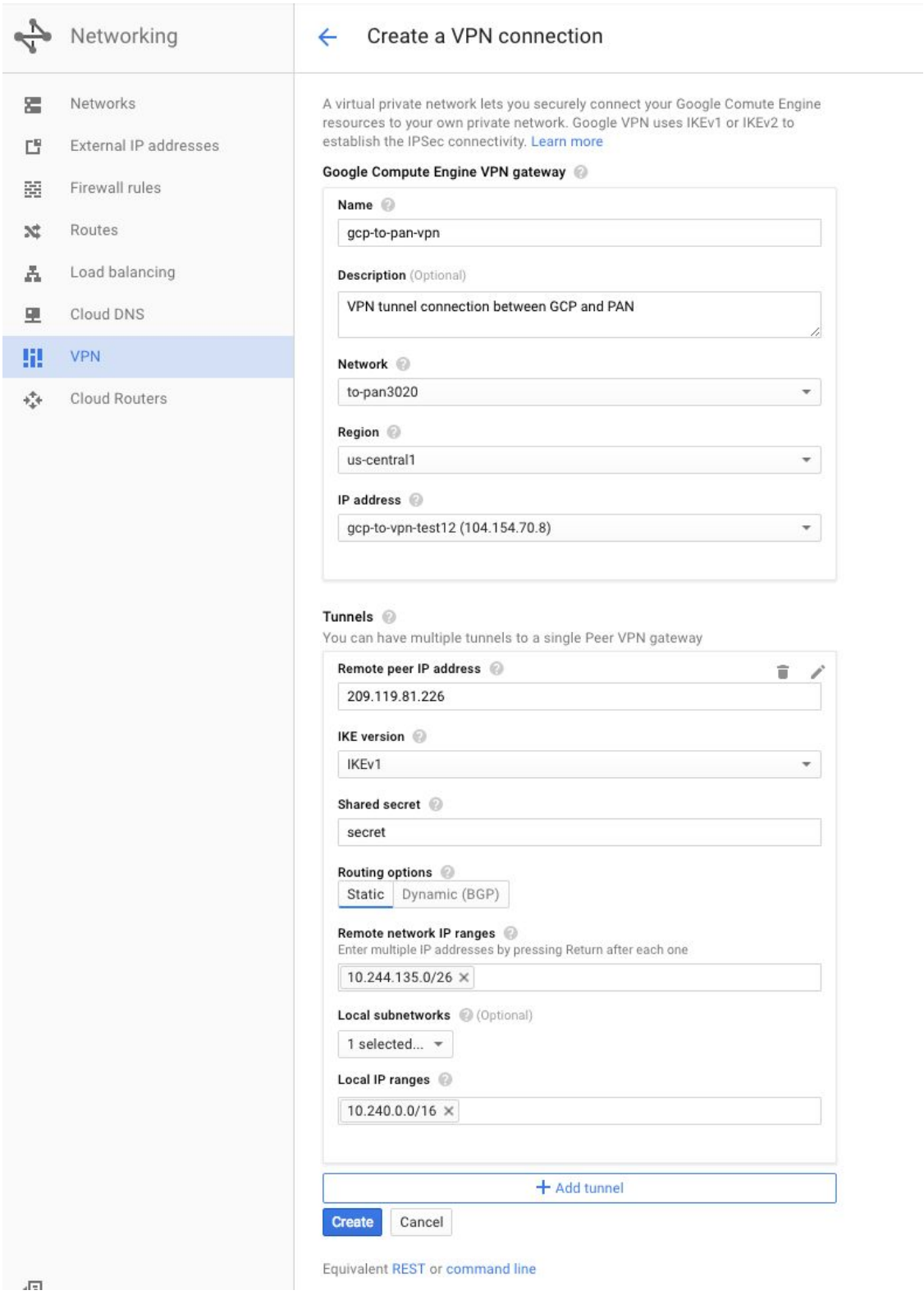
Policy based IPsec VPN setup

Create and configure Cloud VPN

This section provides a step-by-step walkthrough of Google Cloud VPN configuration. Log on to the Cloud console and select Hybrid Connectivity from the main menu. To create a new VPN gateway, select the VPN node under Hybrid Connectivity and click **Create a VPN** from the main task pane:



This page includes all parameters needed to create a new VPN connection. See the following example for a detailed description of each provided parameter.


Networking
Networks
External IP addresses
Firewall rules
Routes
Load balancing
Cloud DNS
VPN
Cloud Routers
Create a 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 VPN gateway
Name
gcp-to-pan-vpn
Description (Optional)
VPN tunnel connection between GCP and PAN
Network
to-pan3020
Region
us-central1
IP address
gcp-to-vpn-test12 (104.154.70.8)
Tunnels
You can have multiple tunnels to a single Peer VPN gateway
Remote peer IP address
209.119.81.226
IKE version
IKEv1
Shared secret
secret
Routing options
Static
Dynamic (BGP)
Remote network IP ranges
Enter multiple IP addresses by pressing Return after each one
10.244.135.0/26
Local subnetworks (Optional)
1 selected...
Local IP ranges
10.240.0.0/16
Add tunnel
Create
Cancel
Equivalent REST or command line

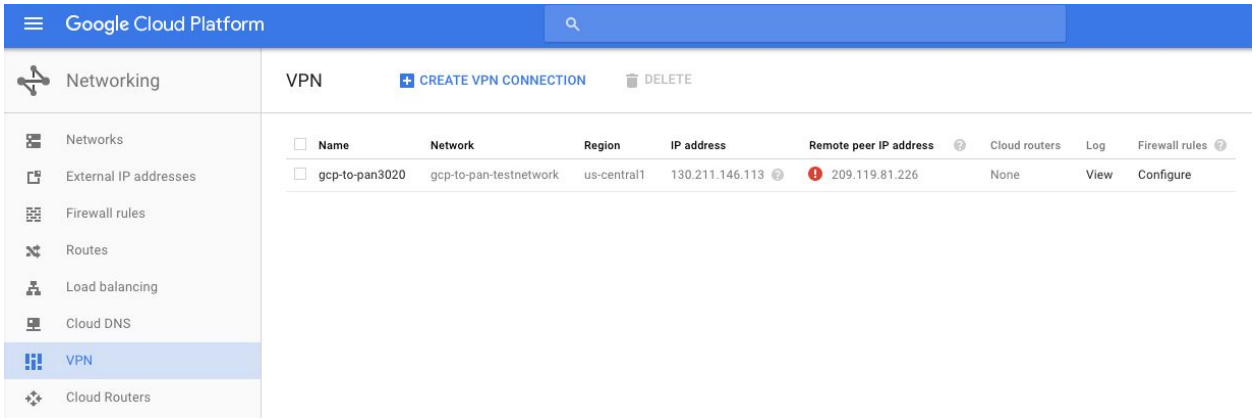
The following parameters are required for the Cloud VPN gateway:

- **Name:** The name of the Cloud VPN gateway.
- **Description:** A brief description of the VPN connection.
- **Network:** the Virtual Private Cloud (VPC) network that the Cloud VPN gateway will attach to. **Note:** This is the VPC network to which VPN connectivity will be made available.
- **Region:** The home region of the Cloud VPN gateway. **Note:** The Cloud VPN gateway must be in the same region as the subnetworks it is connecting.
- **IP address:** The static public IP address that will be used by the Cloud VPN gateway. You can assign an existing, unused, static public IP address within the project, or you can create a new one.

The following parameters are required for each tunnel that is managed by the Cloud VPN gateway:

- **Remote peer IP address:** The public IP address of the on-premises VPN appliance that will 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. Configure the on-premises VPN gateway tunnel using the same shared secret as for the Cloud VPN tunnel..
- **Routing options:** Cloud VPN supports multiple routing options for the exchange of route information between the VPN gateways. This example uses **static routing**. Dynamic routing using Cloud Router and BGP are described in this Fortinet guide.
- **Remote network IP ranges:** The on-premises CIDR blocks being connected to Google Cloud through the Cloud VPN gateway.
- **Local subnetworks:** the Google Cloud CIDR blocks being connected to on-premises through the Cloud VPN gateway.
- **Local IP ranges:** the VPC IP ranges matching the selected subnet.

If the PAN3020 is not set up for VPN tunneling, then you see a “Remote peer IP Address” warning in the VPN dashboard screen. We will configure the PAN3020 in subsequent steps that remove this warning if the setup is successful.



Configuration - gcloud CLI

Cloud VPN can also be configured using the gcloud command-line tool. Command line configuration requires two steps. First you must create the Cloud VPN Gateway, then you must create the tunnels that refer to the Cloud VPN Gateway.

Create the Cloud VPN gateway

```
gcloud compute target-vpn-gateways create gcp-to-pan3020 \
--network gcp-to-pan-testnetwork --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-pan3020 \
--local-traffic-selector gcp-CIDR --remote-traffic-selector on-prem-CIDR
```

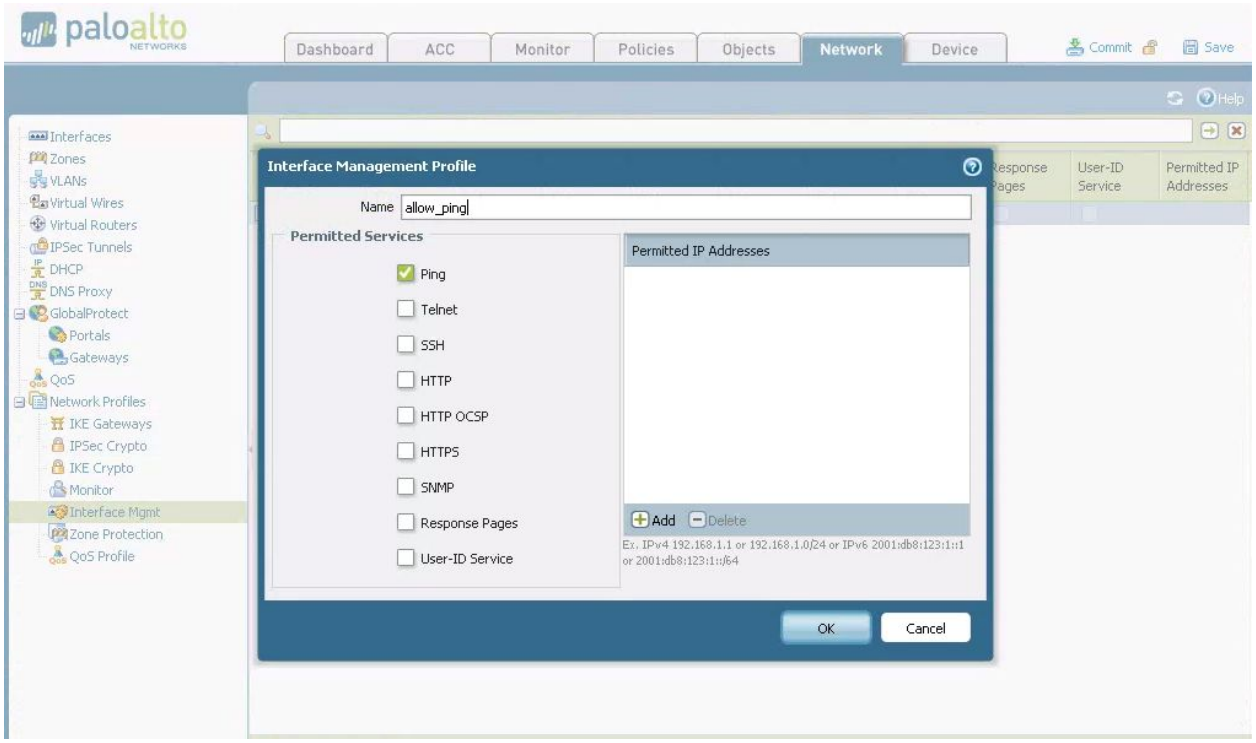
Configuration - Palo Alto network GUI

A VPN tunnel is established after you complete the following steps in the PA-3020 user interface (UI):

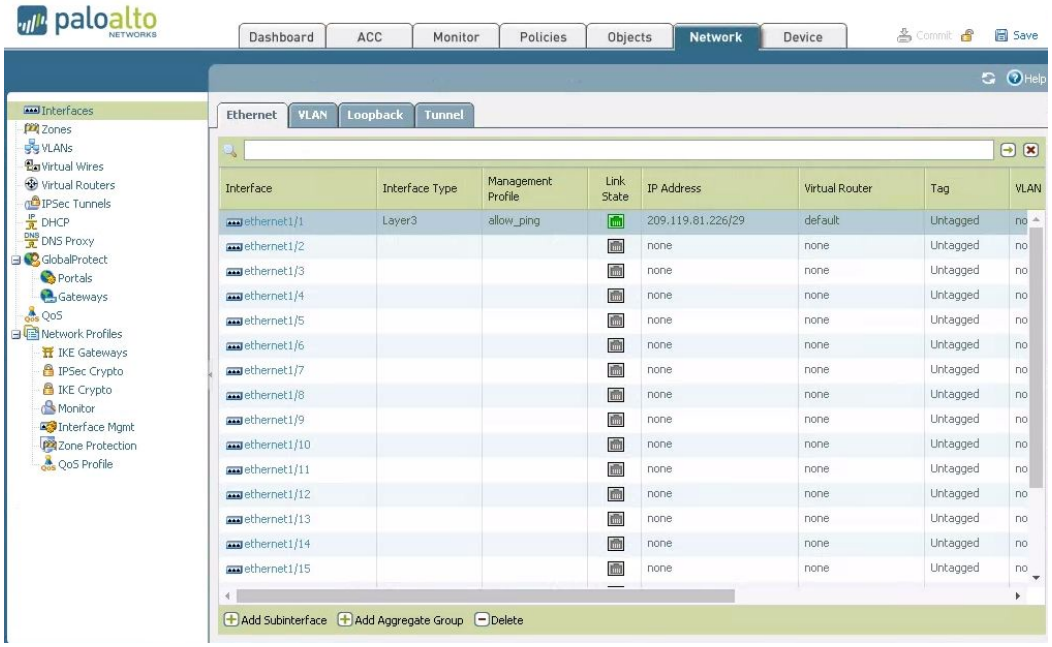
1. Create an Interface Management profile to allow pings
2. Establish an Ethernet Interface with an externally accessible IP address
3. Create a Tunnel Interface
4. Create an IKE profile (Phase 1)
5. Create an IPSec profile (Phase 2)
6. Configure the IKE gateway
7. Configure a virtual router and set a default route
8. Establish an IPSec tunnel with a proxy ID

1. Create an Interface Management profile to allow pings

Select **Add** and give the interface a name (for example, `allow_ping`) and select the checkbox called **ping**. Click **OK**.

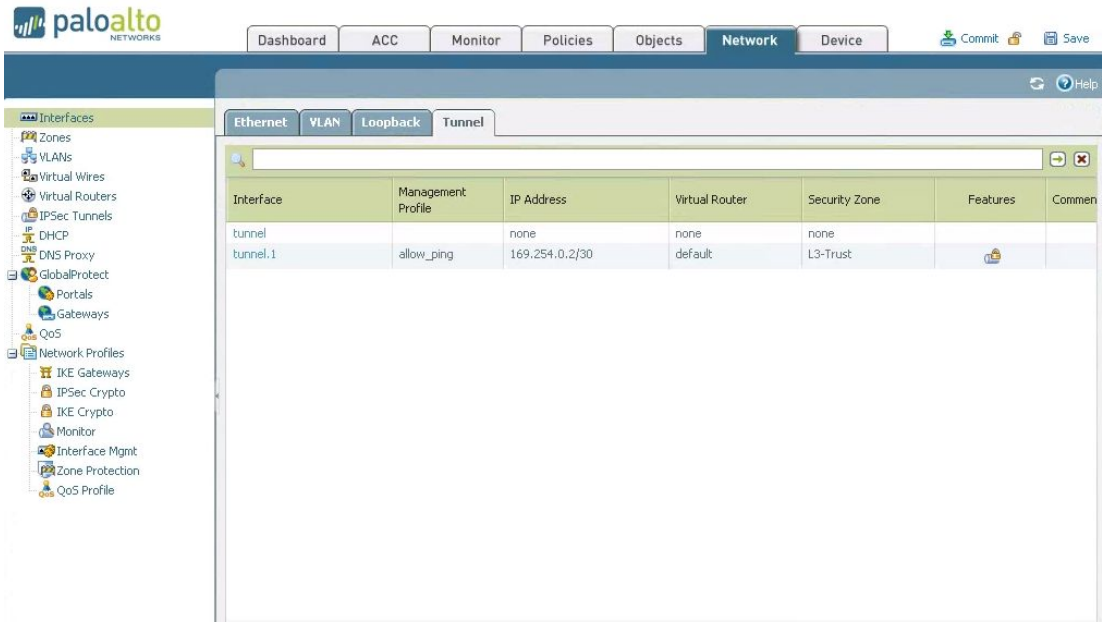


2. Establish an Ethernet Interface with an externally accessible IP



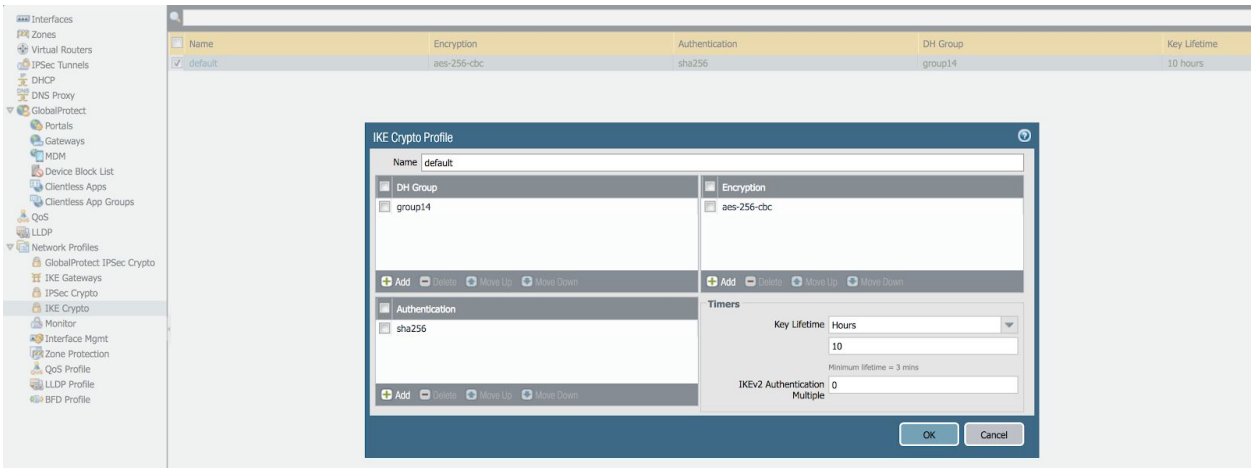
Configure your Ethernet device using the following parameters:
Virtual Router: `default` (will configure later)
Security Zone: `L3-Trust` (Configure under the **Zones** section in the UI)
Interface Type: `Layer 3`
Netflow Profile: `None`
IPv4: An externally accessible IP address. This is the IP address that Cloud VPN uses to establish the IKE handshake and to send traffic.

3. Create a Tunnel Interface



Create a Tunnel Interface using the following parameters:
Virtual Router: `default` (will configure later)
Security Zone: `L3-Trust` (Configure under the **Zones** section in the UI)
Netflow Profile: `None`
IPv4: Leave blank

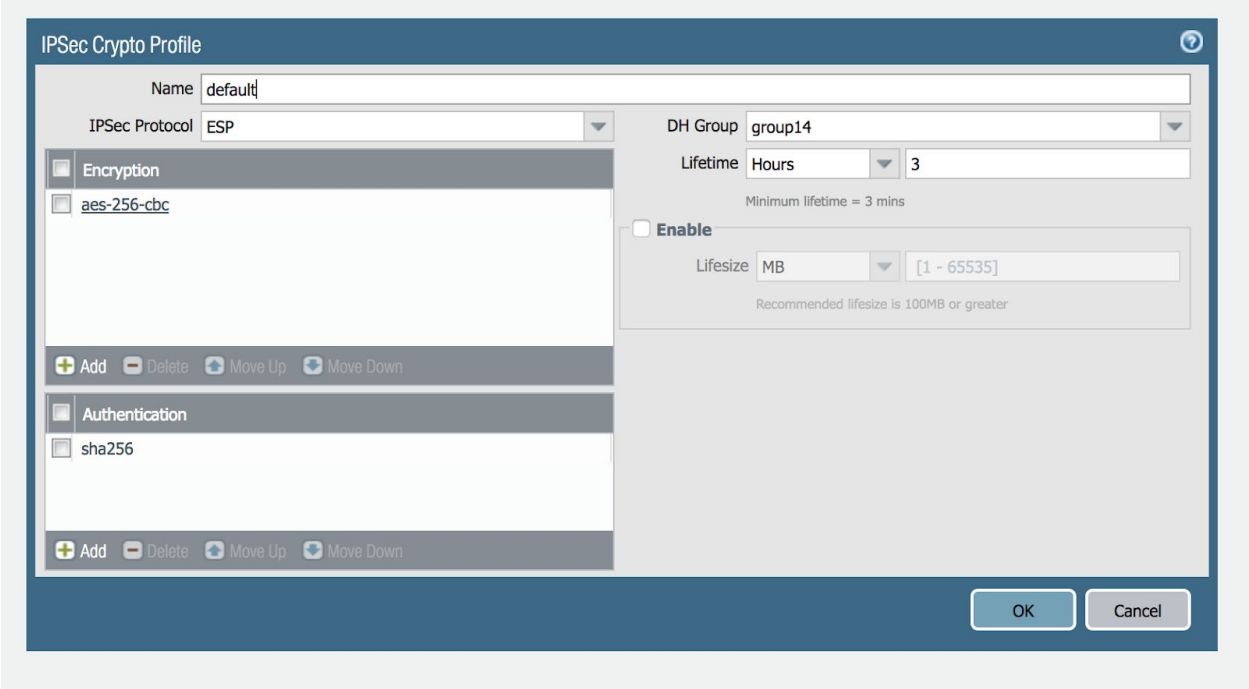
4. Create an IKE profile (Phase 1)



Configure a new IKE Crypto profile (in the example, this profile is named `default`) using the parameters in the above screenshot. It is critically important that these parameters match the configuration on the Cloud VPN side of the tunnel.

Name: `default` (You can use any name you want)
Encryption: `aes-256-cbc`
Authentication: `sha256`
DH Group: `group14`
Lifetime: `10 hours`

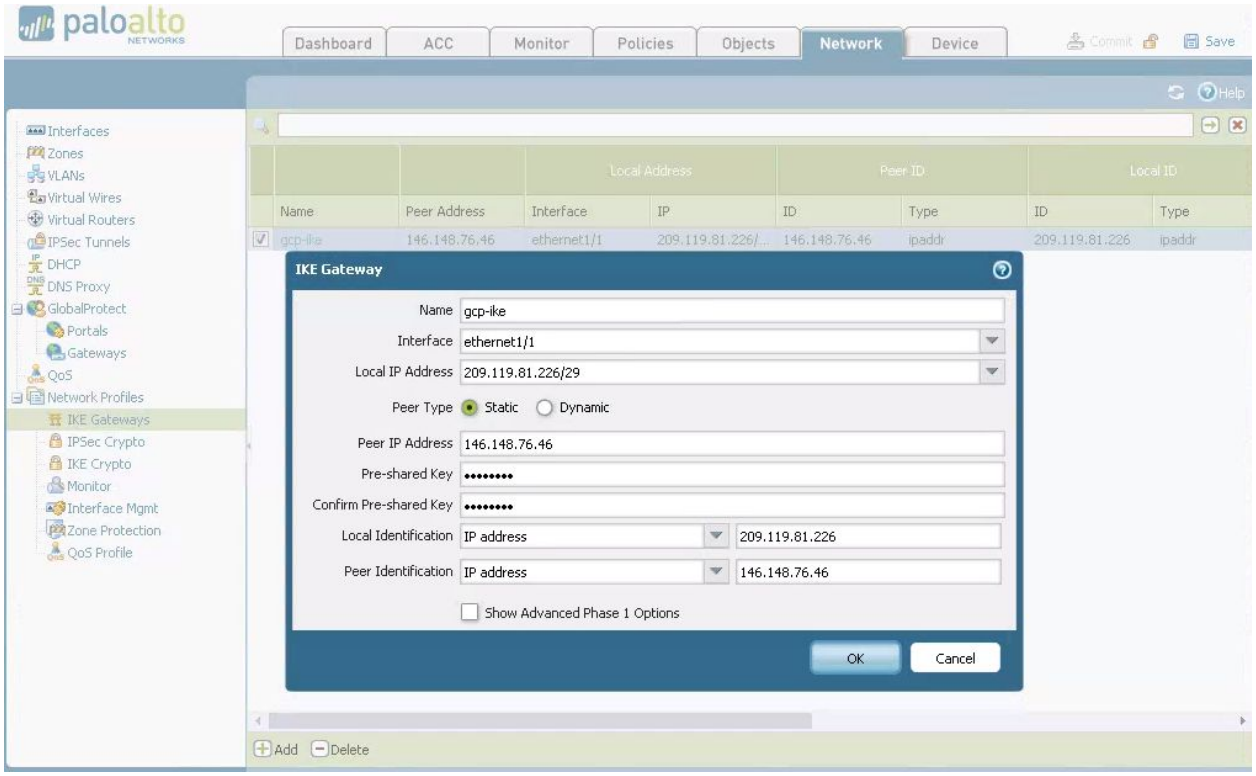
5. Create an IPSec profile (Phase 2)



Configure a new IKE IPSec profile (in the example, this profile is named `default`) using the parameters in the preceding screenshot. It is critically important that these parameters match the configuration on the Cloud VPN side of the tunnel.

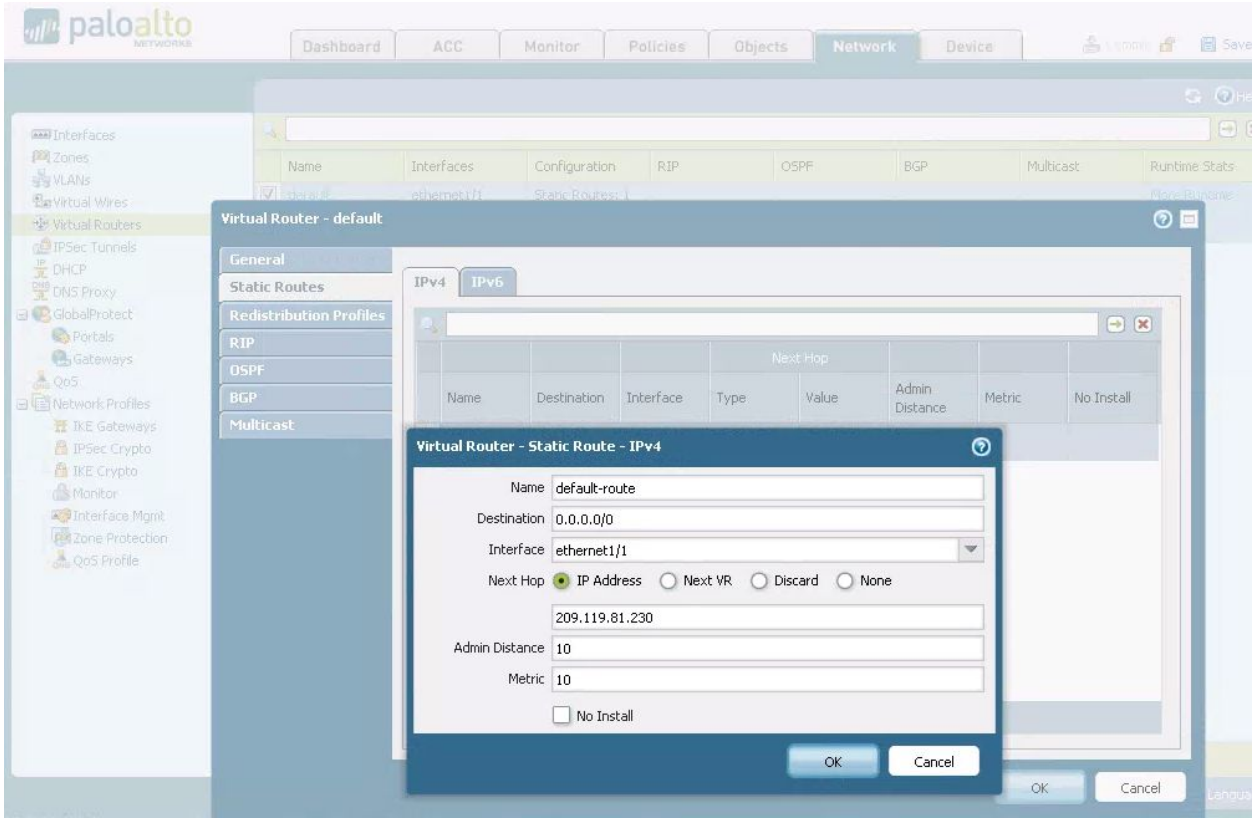
Name: `default` (You can use any name you want)
IPSec Protocol: `ESP`
Encryption: `aes-256-cbc`
Authentication: `sha256`
DH Group: `group14`
Lifetime: `3 hours`

6. Configure the IKE Gateway



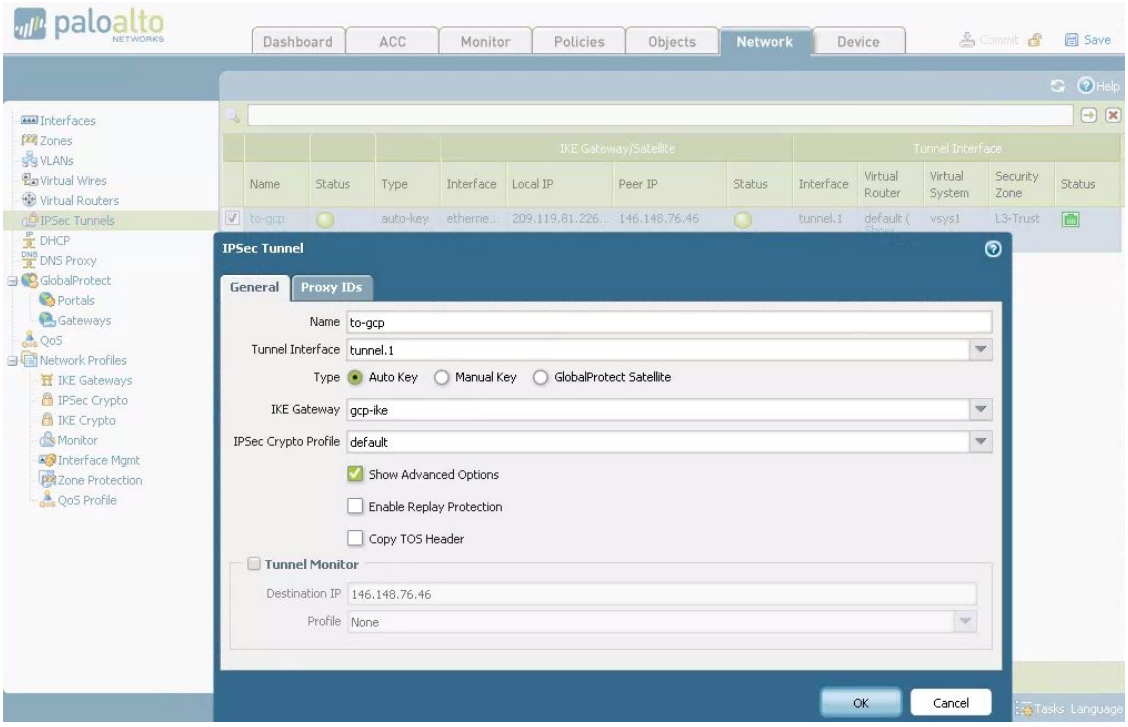
1. The **Interface** field is set to the Ethernet interface that you configured in Step 2.
2. The **Local IP Address** is the IP address that you assigned to that interface.
3. The **Peer IP Address** is the IP address of the VPC network.
4. The **Pre-shared key** is the same key that you configured in the Cloud VPN profile.
5. Set **Local Identification** to the IP address of the ethernet1/1 device.
6. Set **Peer Identification** to the IP address of the peer on the other side of the tunnel.

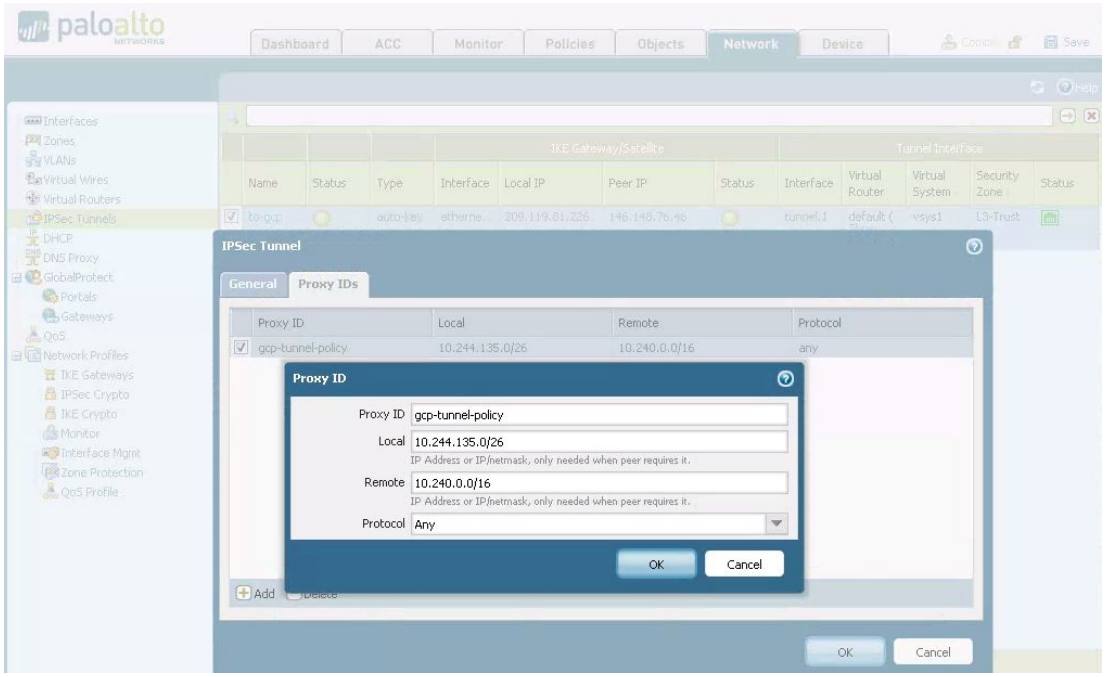
7. Configure a Virtual Router and set a default route



1. Create a new Virtual Router if one does not already exist.
2. Add `ethernet1/1` as the Interface.
3. Create a static route with the parameters illustrated in the screenshot.
4. Set the **Next Hop** as the IP address of the default gateway.

8. Establish an IPSec Tunnel with a proxy ID





1. Set the **Proxy ID** name.
2. The **Local IP address** is the address range of the traffic sent to Google Cloud.

3. The **Remote IP address** is the address range of the traffic sent from Google Cloud.

Test the connection

1. Green status lights indicate a successful connection.
2. In addition, run a ping test from the Palo Alto command line should to verify the connection.

For example:

admin@PA-3020> ping source <*ip address of PAN*> host <*ip address of Cloud VPN*>

Configuration - Palo Alto Network CLI–policy based connection

Follow these steps to establish a VPN tunnel.

1. Establish an Ethernet Interface with an externally accessible IP

```
admin@PA-3020# set network interface ethernet ethernet1/1 layer3 ip
209.119.81.226/29
```

2. Enable ping

```
admin@PA-3020# set network interface ethernet ethernet1/1 layer3
interface-management-profile allow_ping
```

3. Create a tunnel Interface

```
admin@PA-3020# set network interface tunnel units tunnel.1
```

4. Create an IKE profile (Phase 1) (use any name, `default` is used in this example)

```
admin@PA-3020# set network ike crypto-profiles ike-crypto-profiles default
dh-group group14
admin@PA-3020# set network ike crypto-profiles ike-crypto-profiles default
encryption aes-256-cbc
admin@PA-3020# set network ike crypto-profiles ike-crypto-profiles default hash
sha256
admin@PA-3020# set network ike crypto-profiles ike-crypto-profiles default
lifetime hours 10
```

5. Create an IPSec profile (Phase 2) (use any name, `default` is used in this example)

```
admin@PA-3020# set network ike crypto-profiles ipsec-crypto-profiles default
dh-group group14
admin@PA-3020# set network ike crypto-profiles ipsec-crypto-profiles default
esp encryption aes-256-cbc
admin@PA-3020# set network ike crypto-profiles ipsec-crypto-profiles default
esp authentication sha256
admin@PA-3020# set network ike crypto-profiles ipsec-crypto-profiles default
lifetime hours 3
```

6. Configure IKE Gateway (use any name, `gcp-ike` is used in this example)

```
admin@PA-3020# set network ike gateway gcp-ike protocol ikev2
ike-crypto-profile default
admin@PA-3020# set network ike gateway gcp-ike protocol ikev2 exchange-mode
auto
admin@PA-3020# set network ike gateway gcp-ike protocol ikev2 dpd enable yes
admin@PA-3020# set network ike gateway gcp-ike authentication pre-shared-key
key <omitted>
admin@PA-3020# set network ike gateway gcp-ike local-address interface
ethernet1/1
```

```
admin@PA-3020# set network ike gateway gcp-ike peer-address ip 146.148.76.46
admin@PA-3020# set network ike gateway gcp-ike local-id type ipaddr
admin@PA-3020# set network ike gateway gcp-ike local-id id 209.119.81.226
admin@PA-3020# set network ike gateway gcp-ike peer-id type ipaddr
admin@PA-3020# set network ike gateway gcp-ike peer-id id 146.148.76.46
```

7. Configure Virtual Router and set a default route (use any name, “default” was used in this example)

```
admin@PA-3020# set network virtual-router default interface ethernet1/1
admin@PA-3020# set network virtual-router default interface tunnel.1

admin@PA-3020# set network virtual-router default routing-table ip static-route
default-route interface ethernet1/1

admin@PA-3020# set network virtual-router default routing-table ip static-route
default-route  metric 10

admin@PA-3020# set network virtual-router default routing-table ip static-route
default-route destination 0.0.0.0/0 nexthop ip-address 209.119.81.126
```

8. Establish IPSec Tunnel with Proxy ID (use any name, “to-gcp” was used in this example)

```
admin@PA-3020# set network tunnel ipsec to-gcp auto-key ike-gateway gcp-ike
admin@PA-3020# set network tunnel ipsec to-gcp auto-key ipsec-crypto-profile
default
admin@PA-3020# set network tunnel ipsec to-gcp tunnel-monitor enable no
admin@PA-3020# set network tunnel ipsec to-gcp tunnel-interface tunnel.1
admin@PA-3020# set network tunnel ipsec to-gcp auto-key proxy-id
gcp-tunnel-policy local 10.244.135.0/26
set network tunnel ipsec to-gcp auto-key proxy-id gcp-tunnel-policy remote
10.240.0.0/16
```

Configuration - Palo Alto Network CLI BGP

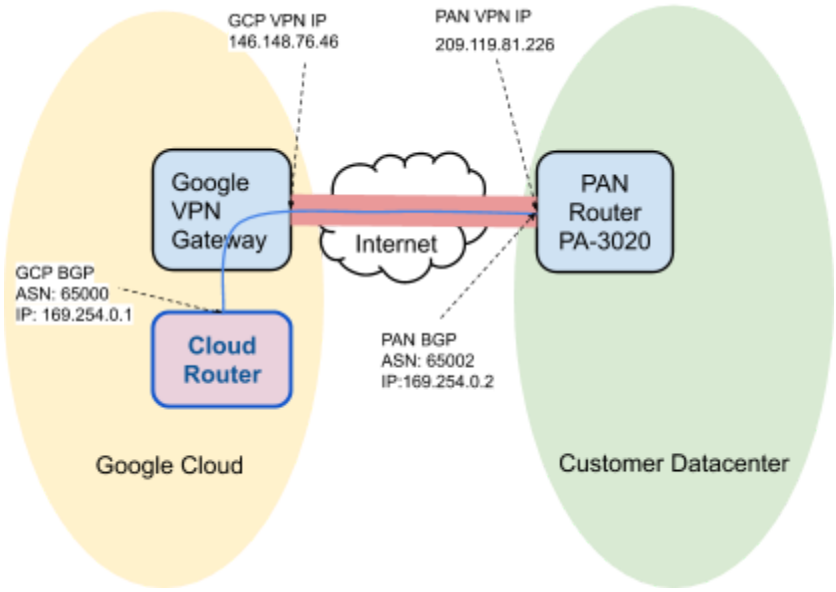
Outline

1. Requirements

This section describes steps to set up BGP interoperability between Cloud VPN and the Palo Alto Networks (PAN-3020) router on your premises.

Note: All IP Addresses used in the following sections are examples only.

2. Setup diagram



3. GCP setup

Create a project in the GCP Cloud Console.

3.1 Cloud VPN and Cloud Router setup

To complete the set up for Cloud VPN and Cloud Router, follow these steps for setting up a Classic VPN using dynamic routing.

4. PAN setup

This section describes how to configure the PAN device for BGP. Each section provides example commands or command output.

4.1 Access

Log into the PAN console.

Console:

```
$ ssh -o PubKeyAuthentication=no -l cloud:7002 100.107.160.100
cloud:7002@100.107.160.100's password:<password>

******
You are now connected to the target.
******

PA-3020 login: admin
Password: <password>
Last login: Thu Jun  9 19:11:46 on ttyS0
Welcome admin.
admin@PA-3020>
```

GUI: http://10.244.135.189/php/login.php (admin/<password>)

4.2 Public IP setup

1. Set up the public IP address on `ethernet1/1` and allow ping.

```
admin@PA-3020# show network interface ethernet ethernet1/1 layer3
layer3 {
  ip {
    209.119.81.226/29;
  }
  interface-management-profile allow_ping;
}
```

2. Set up the default route.

```
admin@PA-3020# show network virtual-router default routing-table ip
static-route default-route
default-route {
  nexthop {
    ip-address 209.119.81.230;
  }
  metric 10;
  destination 0.0.0.0/0;
}
```

3. Add `ethernet1/1` to the default `virtual-router`.

```
admin@PA-3020# set network virtual-router default interface ethernet1/1
```

4. Set up a L3-Trust zone for this interface from the GUI (The CLI command is not documented here).
5. Create a management profile allowing ping on this interface (The CLI command is not documented here).
6. From another device, ping this device on its Public IP address.

4.3 Tunnel Interface setup

1. Set up a tunnel interface. This is the BGP endpoint on the PAN device.

```
admin@PA-3020# show network interface tunnel
tunnel {
  units {
    tunnel.1 {
      ipv6 {
        enabled no;
        interface-id EUI-64;
      }
      ip {
        169.254.0.2/30;
      }
      interface-management-profile allow_ping;
    }
  }
}
```

2. Add the tunnel interface to the default `virtual-router`.

```
admin@PA-3020# set network virtual-router default interface tunnel.1
```

4.4 IKE profile

Set up IKE ciphers.

```
admin@PA-3020# show network ike crypto-profiles ike-crypto-profiles
default
default {
  encryption aes-256-cbc;
  hash sha256;
  dh-group group14;
  lifetime {
    hours 10;
  }
}
```

4.5 IPSec profile

Set up the IPSec profile.

```
admin@PA-3020# show network ike crypto-profiles ipsec-crypto-profiles
ipsec-crypto-profiles {
  default {
    esp {
      encryption aes-256-cbc;
      authentication sha256;
    }
    dh-group group14;
    lifetime {
      hours 3;
    }
  }
}
```

4.6 IKE gateway

Set up the IKE gateway.

```
admin@PA-3020# show network ike gateway
gateway {
  gcp-ike {
    protocol {
      ikev1 {
        dpd {
          enable yes;
          interval 5;
```

```
          retry 5;
        }
        ike-crypto-profile default;
        exchange-mode auto;
      }
    }
    authentication {
      pre-shared-key {
        key -AQ==0YqslrkFtLPIOYkbepHJQUFJUUw=kvL7m4bbTOvtUbnT5xXZKg==;
      }
    }
    protocol-common {
      nat-traversal {
        enable no;
      }
      passive-mode no;
    }
    local-address {
      ip 209.119.81.226/29;
      interface ethernet1/1;
    }
    peer-address {
      ip 146.148.76.46;
    }
  }
}
```

4.7 IPSec tunnel

Set up the IPSec tunnel.

```
admin@PA-3020# show network tunnel
tunnel {
  ipsec {
    gcp-tunnel {
      auto-key {
        ike-gateway {
          gcp-ike;
        }
        ipsec-crypto-profile default;
        proxy-id {
          proxy-id {
            protocol {
              any;
            }
            local 0.0.0.0/0;
```

```
            remote 0.0.0.0/0;
          }
        }
      }
      tunnel-monitor {
        enable no;
      }
      anti-replay no;
      copy-tos no;
      tunnel-interface tunnel.1;
    }
  }
  global-protect-gateway;
}
```

4.8 BGP setup

1. Set up the BGP configuration.

```
admin@PA-3020# show network virtual-router default protocol bgp
bgp {
  enable yes;
  router-id 209.119.81.226;
  local-as 65002;
  redist-rules {
    redistribution {
      address-family-identifier ipv4;
      route-table unicast;
      enable yes;
      set-origin incomplete;
  peer-group {
    vingo-gcp {
      peer {
        vingo-gcp-bgp {
          connection-options {
            keep-alive-interval 20;
            hold-time 60;
          }
          enable yes;
          local-address {
            ip 169.254.0.2/30;
            interface tunnel.1;
          }
          peer-as 65000;
          peer-address {
            ip 169.254.0.1;
```

```
          }
        }
      }
    }
  }
}
```

2. Add a route to the peer BGP endpoint.

```
admin@PA-3020# show network virtual-router default protocol
redist-profile
redist-profile {
  redistribution {
    filter {
      destination 10.244.135.0/26;  -----> "On Prem Private route"
    }
    priority 10;
    action {
      redist;
    }
  }
}
```