Google Cloud VPN Interop Guide
Using Cloud VPN with A Palo Alto Networks® Firewall
Model: PA-3020
Contents

Introduction
Environment Overview
Topology
Configuration
  Overview
  Getting Started
  IPsec Parameters
  Configuration - GCP
  Current Config:
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 Rev:** 8.1.0

Topology

This guide will describe two Cloud VPN connection topologies:

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

![Diagram of Cloud VPN connection topology 1](image)

2. A site-to-site IPsec VPN tunnel configuration using the Google Cloud Router and BGP
IP Addresses for illustrative purposes only

Configuration

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 Internet Key Exchange (IKE) and IPsec
- 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 the following prerequisite conditions have been met:

- Palo Alto Networks PA-3020 online and functional with no faults detected
- Root access to the Palo Alto Networks PA-3020
- At least one configured and verified functional internal interface
- One configured and verified functional external interface

IPsec Parameters

For the PAN-3020 IPsec configuration, the following details will be used:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPsec Mode</td>
<td>ESP+Auth Tunnel mode (Site-to-Site)</td>
</tr>
<tr>
<td>Auth Protocol</td>
<td>Pre-shared Key</td>
</tr>
<tr>
<td>Key Exchange</td>
<td>IKEv2</td>
</tr>
<tr>
<td>Start</td>
<td>auto</td>
</tr>
<tr>
<td>Perfect Forward Secrecy (PFS)</td>
<td>on</td>
</tr>
<tr>
<td>Dead Peer Detection (DPD)</td>
<td>aggressive</td>
</tr>
</tbody>
</table>
The IPsec configuration used in this guide is specified below:

<table>
<thead>
<tr>
<th>Phase</th>
<th>Cipher Role</th>
<th>Cipher</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Phase 1</strong></td>
<td>Encryption</td>
<td>aes-256</td>
</tr>
<tr>
<td></td>
<td>Integrity</td>
<td>sha-256</td>
</tr>
<tr>
<td></td>
<td>prf</td>
<td>sha1-96</td>
</tr>
<tr>
<td></td>
<td>Diffie-Hellman (DH)</td>
<td>Group 14</td>
</tr>
<tr>
<td></td>
<td>Phase 1 lifetime</td>
<td>36,000 seconds (10 hours)</td>
</tr>
<tr>
<td><strong>Phase 2</strong></td>
<td>Encryption</td>
<td>aes-cbc-256</td>
</tr>
<tr>
<td></td>
<td>Integrity</td>
<td>sha-256</td>
</tr>
</tbody>
</table>
Policy Based IPsec VPN Setup

Create and Configure GCP VPN

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:

![Image of Google Cloud Platform Developers Console with VPN creation option]

All parameters needed to create a new VPN connection are entered on this page. A detailed description of each parameter is provided below:
A virtual private network lets you securely connect your Google Compute Engine resources to your own private network. Google VPN uses IKEv1 or IKEv2 to establish the IPsec connectivity. 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-pan-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 subnets** (Optional)
1 selected...

**Local IP ranges**
10.240.0.0/16

Equivalent [REST](https://cloud.google.com/compute/docs/reference/rest/) or [command line](https://cloud.google.com/compute/docs/cli-reference/)
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 with 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 later in this guide.
- **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

If the PAN3020 is not set up for VPN tunneling, you will see a “Remote peer IP Address” warning in the VPN dashboard screen. We will set up the PAN3020 in subsequent steps which will remove the warning if setup is successful.
Configuration - GCP CLI

Cloud VPN can also be configured using the \texttt{gcloud} command line tool. 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

\texttt{gcloud compute target-vpn-gateways create gcp-to-pan3020 --network gcp-to-pan-testnetwork --region us-central1}

Create the VPN Tunnel

\texttt{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 following these sequence of instructions:
1. Create an Interface Management profile to allow pings
2. Establish an Ethernet Interface with an externally accessible IP
3. Create a Tunnel Interface
4. Create an IKE profile (Phase 1)
5. Create an IPSec profile (Phase 2)
6. Configure IKE Gateway
7. Configure Virtual Router and set a default route
8. Establish IPSec Tunnel with Proxy ID
1. Create an Interface Management profile to allow pings

Select Add and give the interface a name (ie. allow_ping) and select the “ping” check box:
2. Establish an Ethernet Interface with an externally accessible IP

Configure your ethernet device with:

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 will be the IP address used by GCP VPN to establish the IKE handshake and to send traffic
3. Create a Tunnel Interface

Use 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, it is named “default”) with the parameters in the above screenshot. It is critically important that these parameters match what is setup on the GCP VPN side of the tunnel.

**Name:** default (could name this anything)

**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, it is named “default”) with the parameters in the above screenshot. It is critically important that these parameters match what is setup on the GCP VPN side of the tunnel.

**Name:** default (could name this anything)

**IPSec Protocol:** ESP

**Encryption:** aes-256-cbc

**Authentication:** sha256

**DH Group:** group14

**Lifetime:** 3 hours
6. Configure IKE Gateway

The Interface field is set to the ethernet interface that was setup in step 2 and the local IP Address is the IP address that is assigned to that interface.

The Peer IP Address is the IP address of the Cloud VPN network while the pre-shared key is what was setup in the Cloud VPN profile.

**Local Identification:** Set to the IP address of the ethernet1/1 device
**Peer Identification:** Set to the IP address of the peer on the other side of the tunnel
7. Configure Virtual Router and set a default route

Create a new Virtual Router if one does not already exist.
Add the ethernet1/1 to the interface

Create a static route with the parameters illustrated in the screenshot

**Next Hop:** IP address of the default gateway
8. Establish IPSec Tunnel with Proxy ID

Set the Proxy ID information. The Local IP address is the address range of the traffic sent to GCP. The Remote IP address is the address range of the traffic sent from GCP.
Test the connection

A successful connection will have green lights to indicate a successful connection. A ping test from the Palo Alto command line should be used to verify the connection as well:

Example:

`admin@PA-3020> ping source <ip address of PAN> host <ip address of Cloud VPN>`
A VPN tunnel is established after following these sequence of instructions:

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
   ```

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

2. Create a Tunnel Interface
   ```
   admin@PA-3020# set network interface tunnel units tunnel.1
   ```

3. Create an IKE profile (Phase 1) (use any name, “default” was 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
   ```

4. Create an IPSec profile (Phase 2)(use any name, “default” was 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
   ```

5. Configure IKE Gateway (use any name, “gcp-ike” was 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**
2. **Setup Diagram**
3. **GCP Setup**
   3.1. **VPN Setup**
   3.2. **Cloud Router Setup**
4. **PAN Setup**
   4.1. **Access**
   4.2. **Public IP Setup**
   4.3. **Tunnel Interface Setup**
   4.4. **IKE Profile Setup**
   4.5. **IPSec Profile Setup**
   4.6. **IKE Gateway Setup**
   4.7. **IPSec Tunnel Setup**
   4.8. **BGP Setup**

1. **Requirements**

   The purpose of this section is to capture instructions for the VPN+BGP interop between GCP and Palo Alto Networks (PAN-3020) router.

   **All IP Addresses are example only**

2. **Setup Diagram**
3. GCP Setup
Create a project on the GCP Cloud Console

3.1 GCP VPN Setup

3.1 GCP Cloud Router Setup
4. PAN Setup
This section shows all the relevant config on the PAN device.

4.1 Access
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>


4.2 Public IP setup
Ethernet1/1 setup:
admin@PA-3020# show network interface ethernet ethernet1/1 layer3
layer3 {
  ip {
    209.119.81.226/29;
  }
  interface-management-profile allow_ping;
}
Default route setup:
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;
}

Add Ethernet1/1 to default virtual-router:
admin@PA-3020# set network virtual-router default interface ethernet1/1

Setup a L3-Trust zone for this interface from GUI (not sure about the CLI for that). Also create a management profile allowing ping on this interface (not sure about the CLI for that). Now from another device, you should be able to ping this device on its Public IP

4.3 Tunnel Interface setup
Setup 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;
        }
    }
}

Add tunnel interface to default virtual-router:
admin@PA-3020# set network virtual-router default interface tunnel.1

4.4 IKE Profile
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
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
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==0YqslrkFtLPIOYkbebHJQUFJUw=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

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

BGP config:

admin@PA-3020# show network virtual-router default protocol bgp
bgp {
enable yes;
router-id 209.119.81.226;
local-as 65002;
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;
        }
      }
    }
  }
}
}

Add route to peer's BGP endpoint:
admin@PA-3020# show network virtual-router default routing-table ip
static-route bgp-route
bgp-route {
  interface tunnel.1;
  metric 10;
  destination 169.254.0.0/30;
}