GOOGLE CLOUD PLATFORM
BYOL INSTANCE QUICK START GUIDE

Introduction

The GCP Marketplace BYOL instance is a 64-bit based appliance that is based on Ubuntu LTS (Long Term Support) you can quickly launch on your GCP VPC in order to get your VPN server up and running. To make it more convenient for you to deploy your server in the region closest to you, we currently offer the instance on the GCP Marketplace.

Important notes about the BYOL licensing model

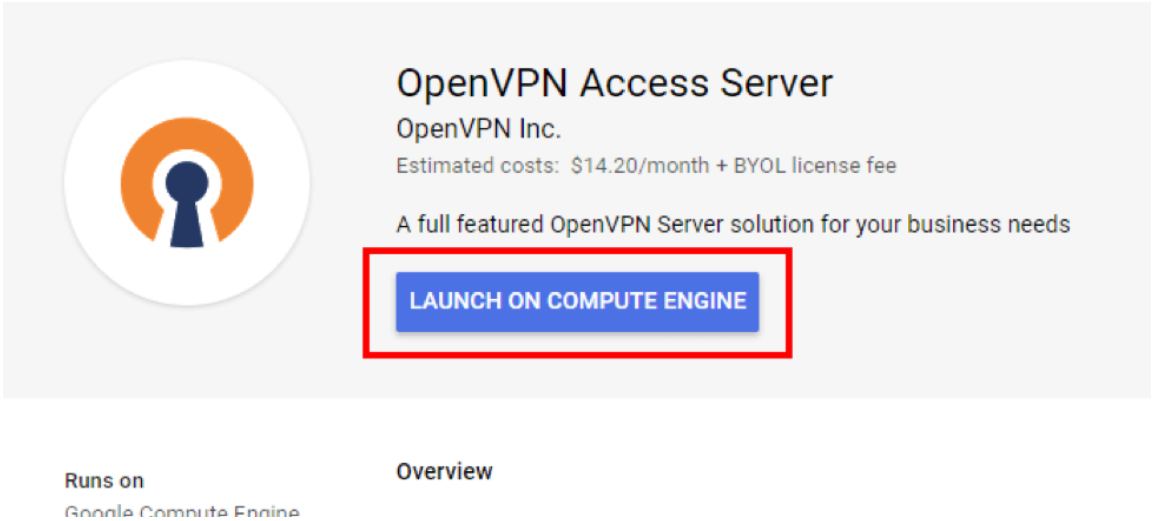
The BYOL (Bring Your Own License) licensing model is one that relies on your purchasing a software license key separately from our openvpn.net website and activating it on your Access Server installation. This locks the key to the current hardware/software configuration on the instance in question. Making changes to the instance like imaging and relaunching it, or changing the instance type, or enabling auto-scaling, will result in the license key becoming invalid, requiring you to contact us for support on this. See our troubleshooting page regarding BYOL type license keys for more information on how to request a license key reissue or check the licensing state of your BYOL type key.

It's also important to note here that when you launch the BYOL type appliance with the instructions given below, then you do not actually need to provide a license key. If you do not provide a license key, the Access Server goes into a type of demonstration mode where all functions are available without time limit, but only 2 simultaneous VPN connections can be made at a time. To unlock more connections, you need to purchase and activate a license key on your Access Server installation.

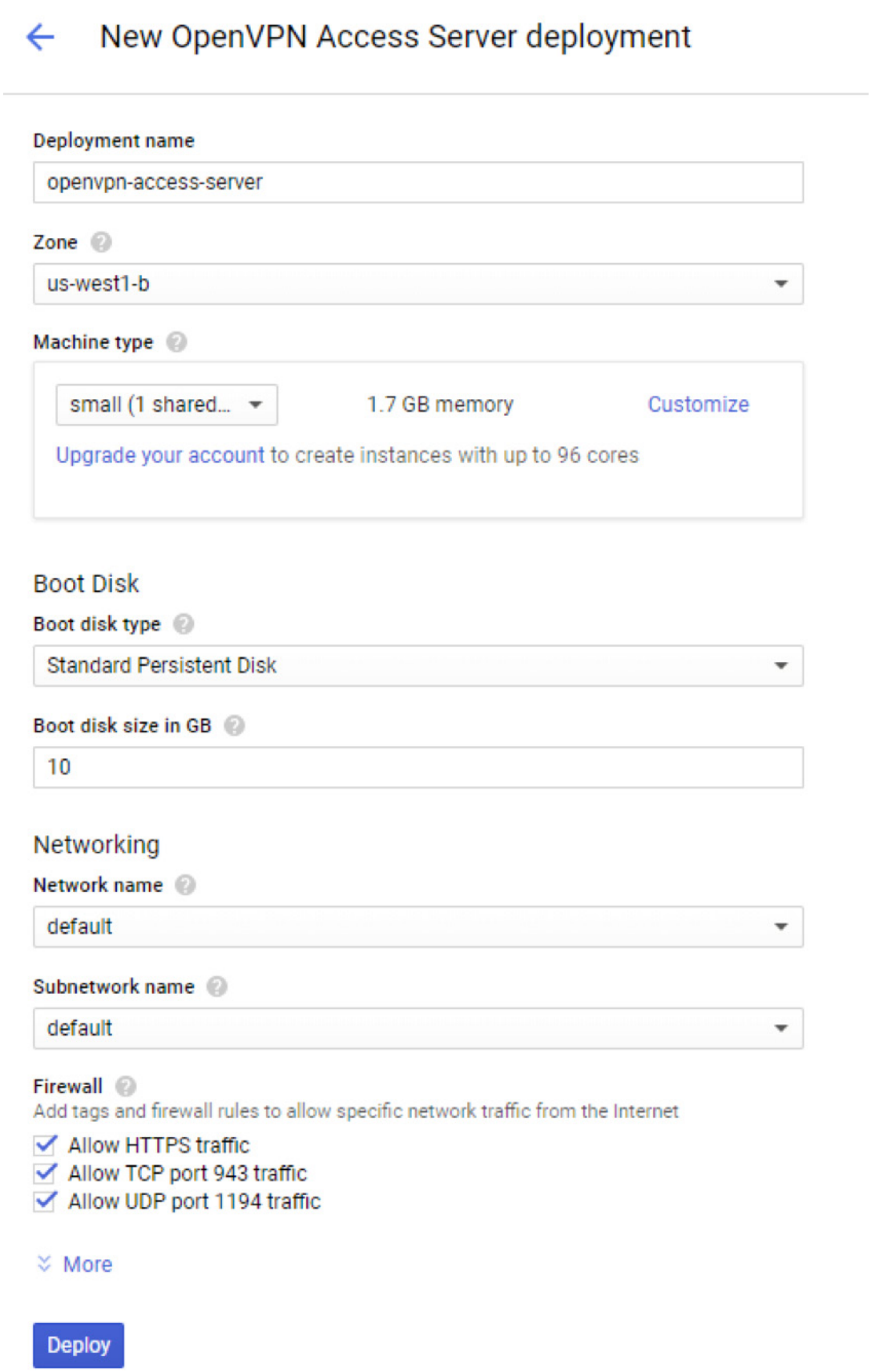
Launching the Appliance

To get started, visit the GCP Marketplace site by clicking here. In the search bar that appears, enter **OpenVPN Access Server** and click the resulting solution that appears.

To launch the instance, click the **Launch on Compute Engine** button, as follows:



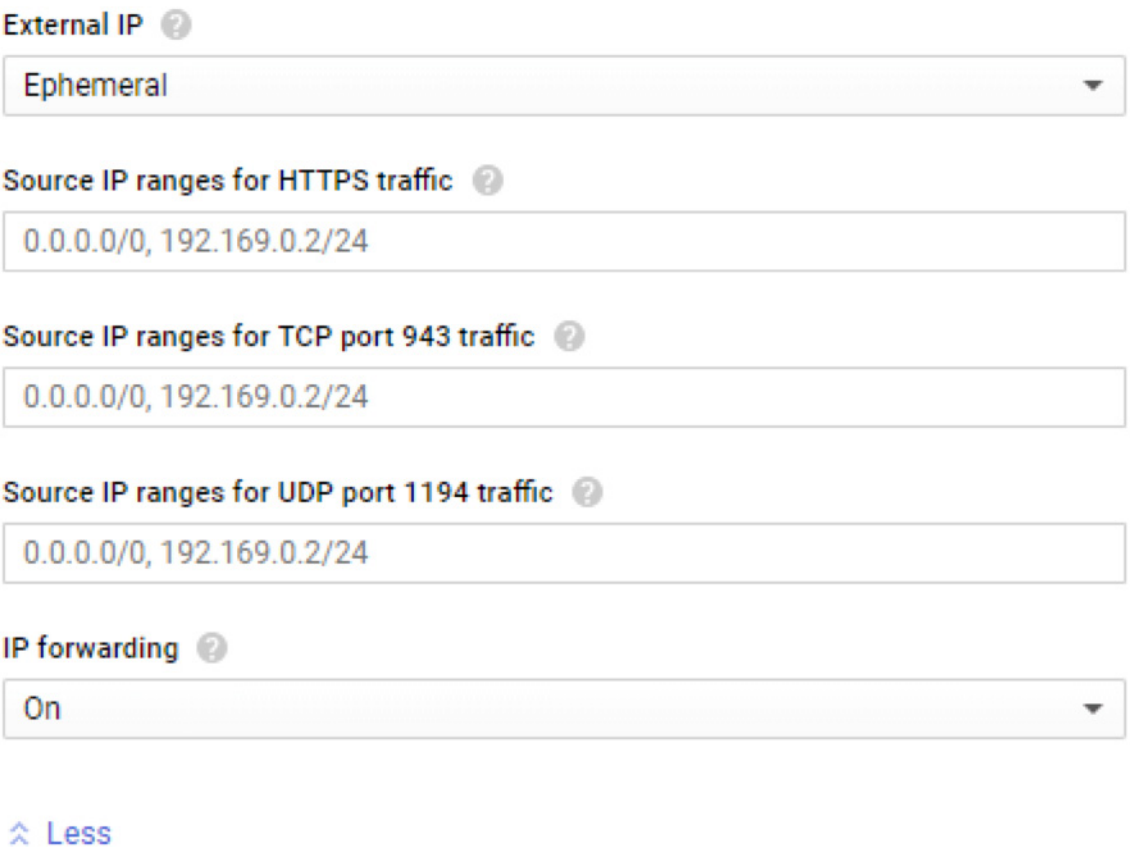
Afterward, follow the instructions below:



Instance Launch Options:

- **Deployment name:** Specify the name of the instance you would like to use.
- **Zone:** Specify the region you would like to launch your VPN server into.
- **Machine type:** The instance type and size for your VPN server. For optimal performance, it is recommended that **small (1 shared vCPU)** is chosen, or better.
- **Boot disk type:** Standard Persistent Disk is appropriate for the VPN instance since there is minimal disk I/O for the instance.
- **Boot disk size in GB:** The instance by default comes with a 10 GB boot disk. You may increase this to a bigger number according to your needs, if necessary.
- **Network name / Subnetwork name:** The network you would like to place your VPN server on. The VPN server needs be placed inside the same network as your other resources for them to be reachable over the VPN network.
- **Firewall:** The firewall rules are already configured for you for this instance. If you would like to restrict access to your instance, please click the **More** link underneath the **Firewall** section to customize IP access rules.

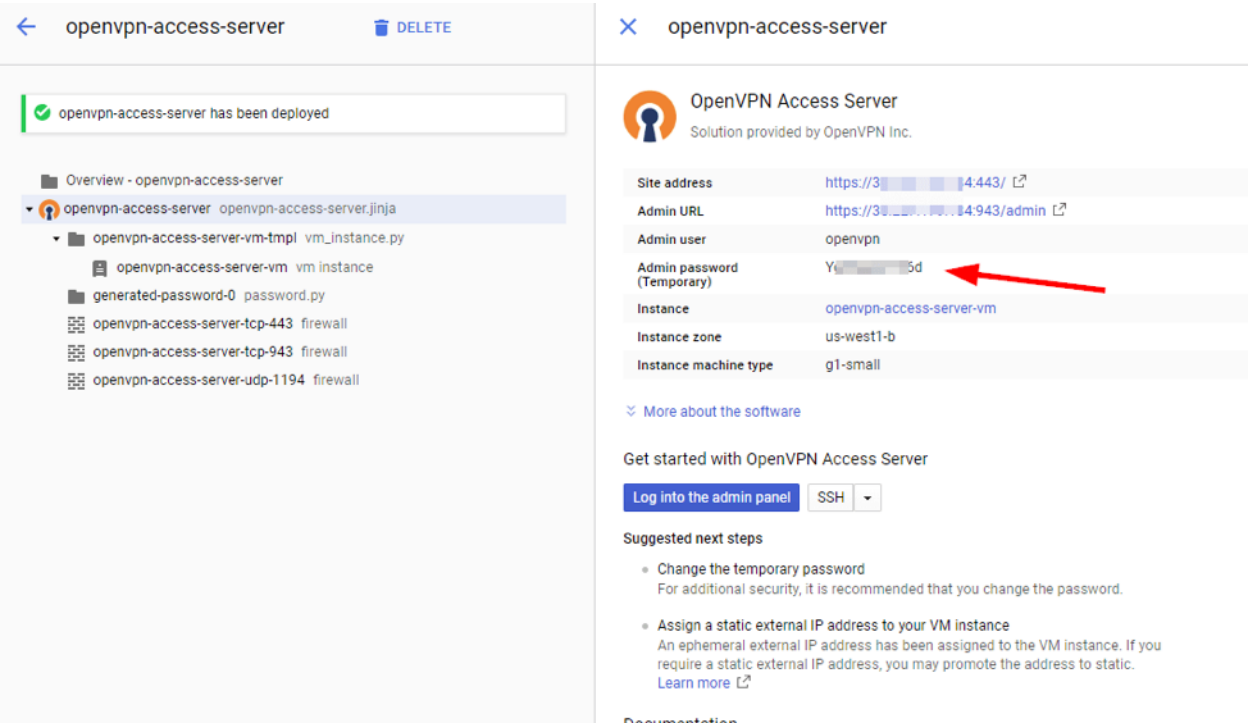
If you click the **More** link below the available firewall rules, the following options are available:



- **External IP:** By default, a dynamic (ephemeral) IP address is available. A static IP can be reserved for the instance at a later step.
- **Source IP ranges for HTTPS traffic:** Define the source IP address ranges that should be allowed to access the TCP daemon for the VPN server. Blocking access to this port will prevent users from connecting to the VPN server using TCP. Please note that by default the administrative portal is available also on this port. You may disable this option in the administrative portal when the instance is deployed.

- **Source IP ranges for TCP port 943 traffic:** Define the source IP address ranges that should be allowed to access the administrative UI on TCP port 943. The range of IP addresses should be limited to your trusted IP ranges whenever possible.
- **Source IP ranges for UDP port 1194 traffic:** Define the source IP address ranges that should be allowed to access the UDP daemon for the VPN server. Blocking access to this port will prevent users from connecting to the VPN server using UDP. Note that UDP is the default mode for the VPN server and the client will automatically failback to using TCP if the UDP protocol is unavailable or blocked.
- **IP forwarding:** This option should remain **On** if you plan to use the VPN server for a site-to-site tunnel. If a site-to-site tunnel is not used or if you only plan to be accessing remote resources via **NAT** mode, then this option may be turned off.

After verifying the instance details, click the **Deploy** button to initiate the launching process. The launching process is expected to take 2-3 minutes, so please be patient while the instance is being instantiated. Once the instance has been created successfully, the wizard should allow you to connect to the instance with a randomly generated password.



IMPORTANT: The **Log into the admin panel** button will allow you to access the administrative interface using HTTPS. However, the instance will present a self-signed certificate when it is first launched. As a result, a browser security error will result when you initially log in to the admin panel. To remove the security error, please upload a trusted SSL certificate under the Web Server admin section upon logging in.

As mentioned in the **Suggested next steps** section, it is important to change the temporary password assigned to this instance once it has been launched. To do so, click the SSH button to access the instance via **SSH**, and use the:

```
sudo passwd openvpn
```

command to change the password for the default administrative user. Use the **Learn more** link to learn how you can promote your ephemeral IP address into a static IP address. This is strongly recommended to ensure that your users can connect to your VPN server as designed.

Changing Default Hostname (Admin UI)

If you have a custom hostname you would like to use, you will need to login to the Web Admin UI and configure the **Hostname** parameter manually (inside the Server Settings section). You may either use an IP address or a hostname here, although it is strongly recommended that you use a hostname since your clients will depend on this setting to be able to know where to connect to, and updating a DNS record is much easier than reinstalling all clients to update the IP address they need to connect to. Also, SSL certificates require a proper FQDN hostname in order to function properly.

Note: This value is by default filled with your initial ephemeral IP address and will have to be changed if you ever change your IP address for your instance.

Changing Default Timezone (SSH)

The default timezone is set to **US (Pacific – Los Angeles)**. If you reside at another timezone and you would like to change this setting, run the following command in SSH (you will be asked what timezone you would like to set):

```
sudo dpkg-reconfigure tzdata
```

The system will show the new local time after this setting is configured.

Install NTP client for automatic time synchronization (SSH)

This is recommended for all situations but especially for people that want to use Google Authenticator.

```
apt-get install ntp
```

Set up static routes if necessary

By default, the OpenVPN Access Server gives VPN clients access to your VPC by using the NAT method (Network Address Translation). Using this method, traffic originating from the VPN clients will appear to be coming from the local IP address of the Access Server. For that reason, routing is not necessary and is much easier to implement. However, one drawback of using such method is that traffic from the VPC itself cannot directly access a VPN client as the NAT engine prevents such direct contact. In order to allow a VPN client to be directly addressable via the VPC, you will need to configure the Access Server to use the routing method instead of NAT. Once that is done, the source IP address of packets coming from the VPN clients is kept intact, and direct access from the VPC network to the VPN client subnet is then possible. However, because the VPC does not automatically recognize the VPN subnet within the VPN instance, it does not know how to send the return traffic back to the instance. To correct this problem, you will need to add a static route in the Google routing table for your VPC so that the return traffic flows properly. To learn how to do this see this document on Google VPC routing:

- https://cloud.google.com/vpc/docs/routes

Note: A site to site VPN tunnel with routing requires the **IP forwarding** option to be turned on when the instance is created. If this option was turned off initially, any static routing within the VPN network will fail. You will need to relaunch your instance with the correct parameter in order to correct this issue.

Updating Operating System Software (recommended)

From the time we have generated the appliance and the time you have downloaded and are using the appliance, operating system updates might have become available. To make sure your appliance operating system is up to date, execute the following commands:

```
sudo apt-get update
sudo apt-get upgrade
```

Further security recommendations

We also have some security recommendations that you should implement as well, which apply to all OpenVPN Access Server installations.

OPENVPN®

7901 Stoneridge Drive, Suite 540
Pleasanton, CA 94588 USA
Sales: sales@openvpn.net
Support: help@openvpn.net

OPENVPN.NET

OVASGoogleCloudQSG1906.v1