Barracuda Web Application Firewall Deployment on Google Cloud Platform via the Google Launcher

https://campus.barracuda.com/doc/76284335/

This section walks you through steps of how to deploy the Barracuda Web Application Firewall (WAF) on Google Cloud Platform via the Google Launcher.

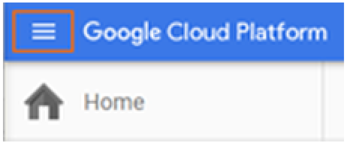
> Ensure that you do not configure the WAF behind a Google TCP load balancer. Always use an HTTP load balancer.

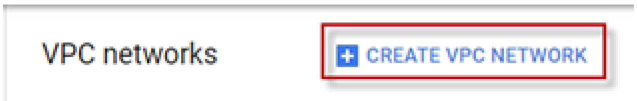
Before You Begin

Ensure that you have a Google account created.

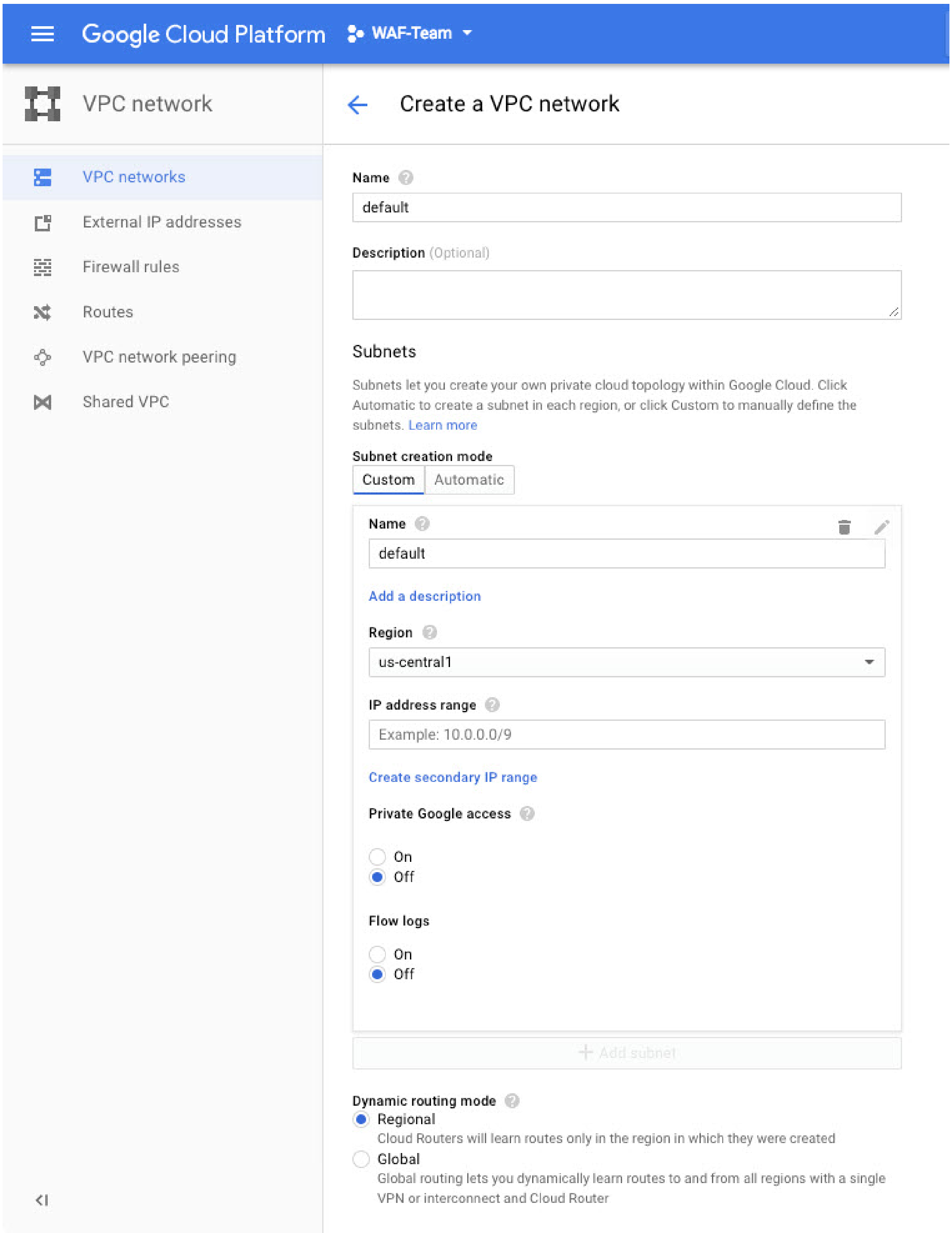
Step 1. Create a Network in the Google Cloud

Create the virtual network you are deploying your firewall to

1. Go to https://console.cloud.google.com.
2. Click the hamburger menu in the upper-left corner.


3. From the **Networking** section, click **VPC networks** and then select **VPC networks** from the list.
4. In the **VPC networks** window, click **Create VPC Network**.


5. In the **Name** and **Description** boxes, specify a name for the network and its description.
6. In the **Subnetworks** section, click **Custom**.
7. Create the public subnet:
    - **Name** - Enter public-subnet
    - **Region** - Select your region.
    - **IP address range** - Enter the network in CIDR format. If possible, do not use a network that overlaps with your on-premises network.



Name

default

Description (Optional)

Subnets

Subnets let you create your own private cloud topology within Google Cloud. Click Automatic to create a subnet in each region, or click Custom to manually define the subnets. Learn more

Subnet creation mode

Custom | Automatic

Name

default

Add a description

Region

us-central1

IP address range

Example: 10.0.0.0/9

Create secondary IP range

Private Google access

○ On
● Off

Flow logs

○ On
● Off

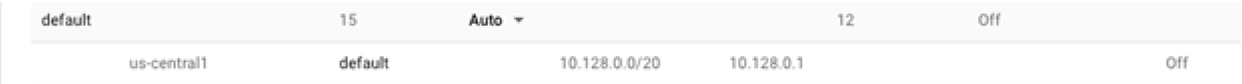
+ Add subnet

Dynamic routing mode

● Regional
Cloud Routers will learn routes only in the region in which they were created

○ Global
Global routing lets you dynamically learn routes to and from all regions with a single VPN or interconnect and Cloud Router

8. Click **Create** . The network is now listed.



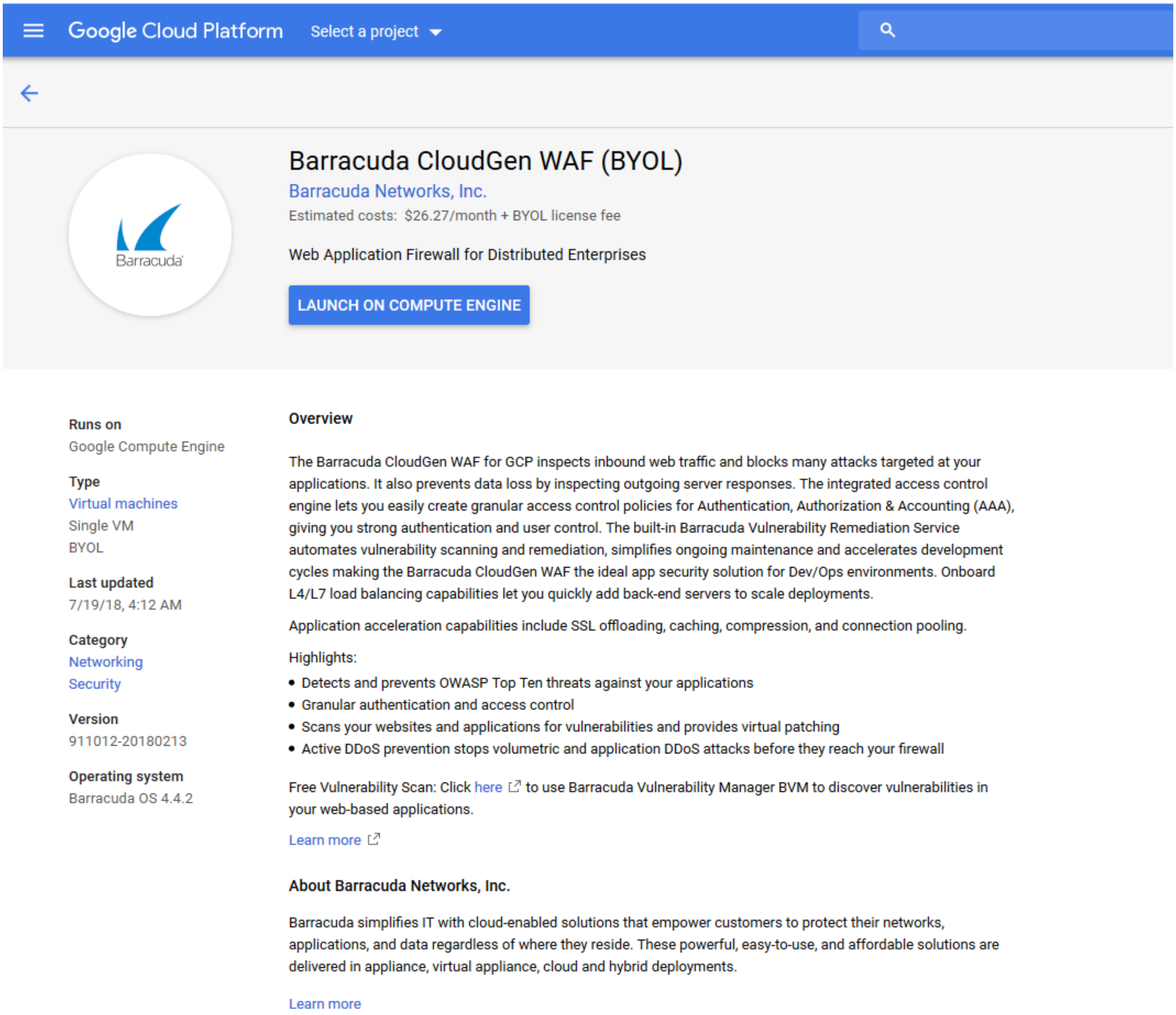
default		15	Auto		12	Off	
	us-central1	default	10.128.0.0/20	10.128.0.1			Off

Step 2. Create the WAF Instance from Cloud Launcher

Deploy a new Barracuda Web Application Firewall (BYOL) instance from the Cloud Launcher image.

You can follow the same steps for deploying the Barracuda Web Application Firewall (PayG) instance on Google Cloud, except for the licensing section that is not required.

1. Go to the Barracuda CloudGen WAF (BYOL) page.
2. Click **Launch on Compute Engine**.



Barracuda CloudGen WAF (BYOL)

Barracuda Networks, Inc.

Estimated costs: $26.27/month + BYOL license fee

Web Application Firewall for Distributed Enterprises

Runs on
Google Compute Engine

Type
Virtual machines
Single VM
BYOL

Last updated
7/19/18, 4:12 AM

Category
Networking
Security

Version
911012-20180213

Operating system
Barracuda OS 4.4.2

Overview

The Barracuda CloudGen WAF for GCP inspects inbound web traffic and blocks many attacks targeted at your applications. It also prevents data loss by inspecting outgoing server responses. The integrated access control engine lets you easily create granular access control policies for Authentication, Authorization & Accounting (AAA), giving you strong authentication and user control. The built-in Barracuda Vulnerability Remediation Service automates vulnerability scanning and remediation, simplifies ongoing maintenance and accelerates development cycles making the Barracuda CloudGen WAF the ideal app security solution for Dev/Ops environments. Onboard L4/L7 load balancing capabilities let you quickly add back-end servers to scale deployments.

Application acceleration capabilities include SSL offloading, caching, compression, and connection pooling.

Highlights:

- Detects and prevents OWASP Top Ten threats against your applications
- Granular authentication and access control
- Scans your websites and applications for vulnerabilities and provides virtual patching
- Active DDoS prevention stops volumetric and application DDoS attacks before they reach your firewall

Free Vulnerability Scan: Click here to use Barracuda Vulnerability Manager BVM to discover vulnerabilities in your web-based applications.

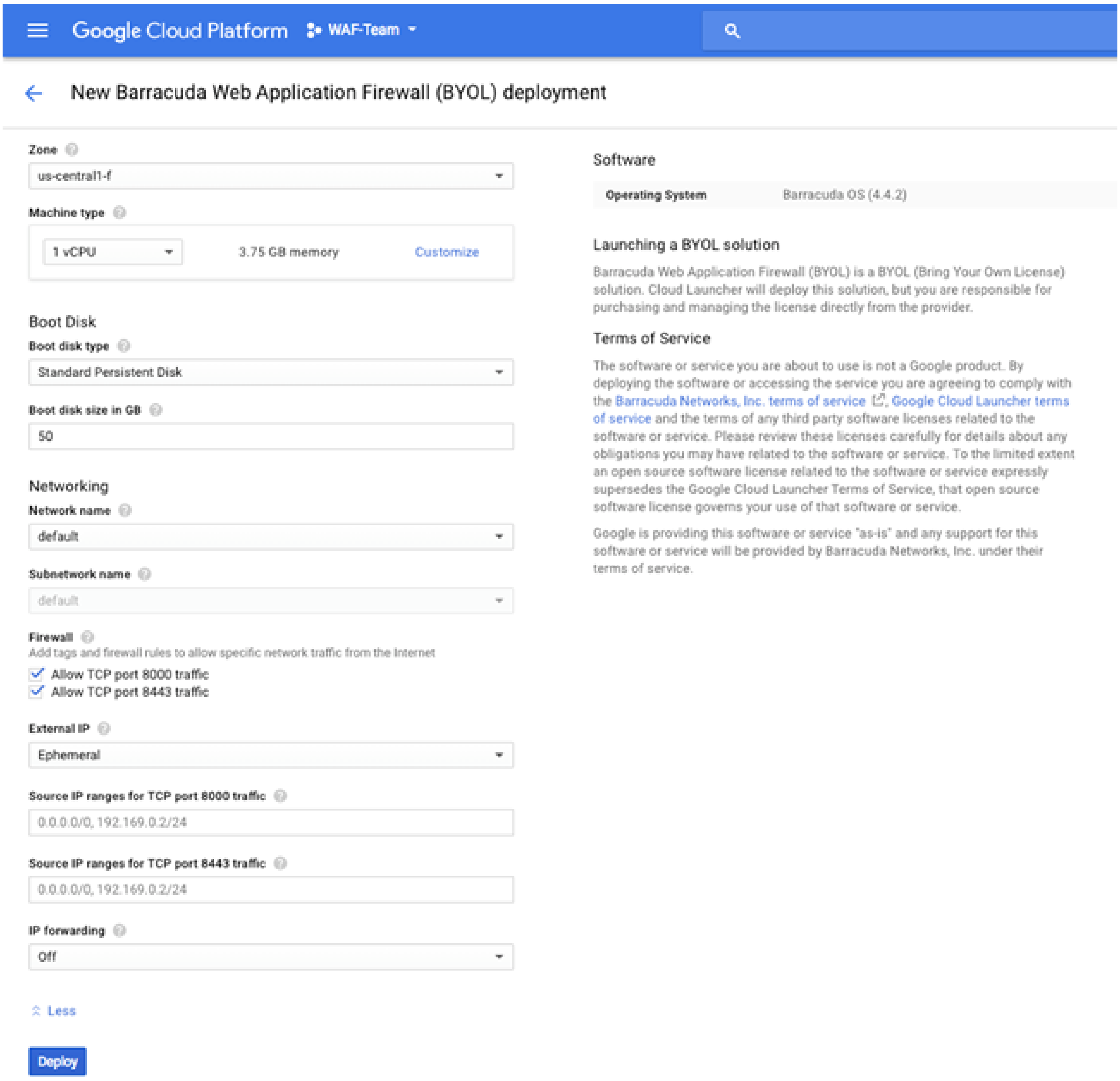
Learn more

About Barracuda Networks, Inc.

Barracuda simplifies IT with cloud-enabled solutions that empower customers to protect their networks, applications, and data regardless of where they reside. These powerful, easy-to-use, and affordable solutions are delivered in appliance, virtual appliance, cloud and hybrid deployments.

Learn more

3. Enter the Deployment name.
4. From the **Zone** list, select the region for your new firewall instance.
5. Select the **Machine type** with the number of vCPUs corresponding to your Barracuda WAF license and performance needs. For more information, see Public Cloud.
6. Change **Disk type** to SSD if you plan to use IO-intensive features like WAN Opt, Malware Protection, or HTTP Proxy. Otherwise, leave the default setting to **Standard Persistent Disk**.
7. In **Networking**, choose network and subnetwork names for the public subnet you created in Step 1.



New Barracuda Web Application Firewall (BYOL) deployment

Zone: us-central1-f

Machine type: 1 vCPU, 3.75 GB memory

Boot Disk

Boot disk type: Standard Persistent Disk

Boot disk size in GB: 50

Networking

Network name: default

Subnetwork name: default

Firewall

Add tags and firewall rules to allow specific network traffic from the Internet

☑ Allow TCP port 8000 traffic
☑ Allow TCP port 8443 traffic

External IP: Ephemeral

Source IP ranges for TCP port 8000 traffic: 0.0.0.0/0, 192.169.0.2/24

Source IP ranges for TCP port 8443 traffic: 0.0.0.0/0, 192.169.0.2/24

IP forwarding: Off

Software

Operating System	Barracuda OS (4.4.2)

Launching a BYOL solution

Barracuda Web Application Firewall (BYOL) is a BYOL (Bring Your Own License) solution. Cloud Launcher will deploy this solution, but you are responsible for purchasing and managing the license directly from the provider.

Terms of Service

The software or service you are about to use is not a Google product. By deploying the software or accessing the service you are agreeing to comply with the Barracuda Networks, Inc. terms of service, Google Cloud Launcher terms of service and the terms of any third party software licenses related to the software or service. Please review these licenses carefully for details about any obligations you may have related to the software or service. To the limited extent an open source software license related to the software or service expressly supersedes the Google Cloud Launcher Terms of Service, that open source software license governs your use of that software or service.

Google is providing this software or service "as-is" and any support for this software or service will be provided by Barracuda Networks, Inc. under their terms of service.

8. Leave all the default firewall positions checked. You can add more ports, protocols, and IP addresses after deployment.
9. (optional) If you want to use a reserved static address as created in Step 2:
    1. Click **More** to expand the advanced options.
    2. Select your **External IP** from the list.
10. Click **Create** to start the deployment.

Step 3 - License the Barracuda Web Application Firewall

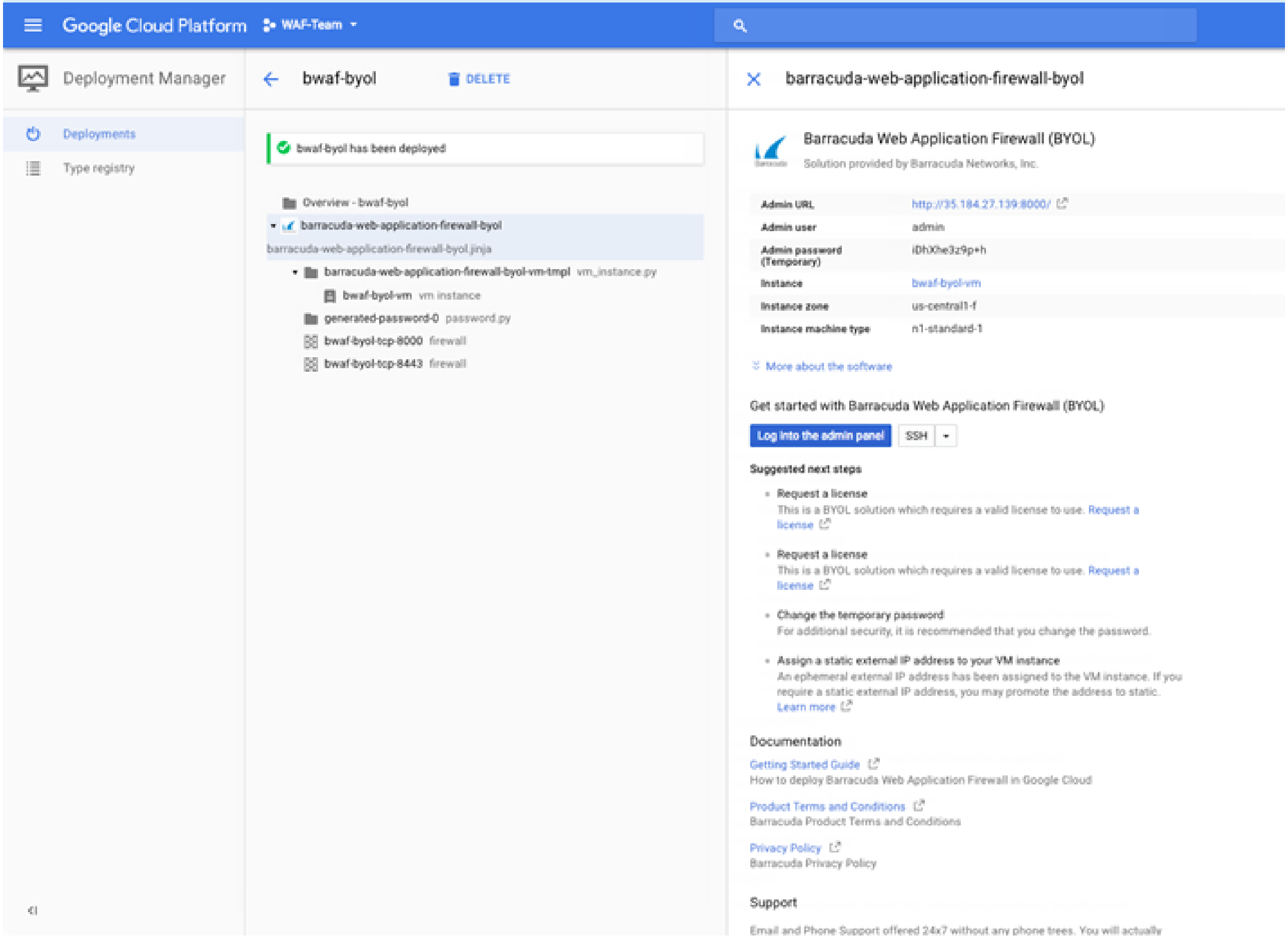
If you have deployed the Barracuda Web Application Firewall with the Hourly option, you do not need to license the system; skip ahead to **Step 7 - Verify Configuration and Change the**

Password

If you have deployed the Barracuda Web Application Firewall with BYOL, complete the licensing and provisioning of your system.

1. Go to https://console.cloud.google.com.
2. Click the hamburger menu in the upper-left corner.
3. From the **Tools** section, click **Deployment Manager** and then select **Deployment** from the list.
4. In the left pane, click the deployment that you have just created**.**
5. In the right pane, click **Log into the admin panel**.

   To access the Barracuda Web Application Firewall from the browser directly, use the following:
   For HTTP: http://<Public DNS>:8000 (Unsecured)
   For HTTPS: https://<Public DNS> (Secured)
   The Barracuda Web Application Firewall is not accessible via the HTTPS port at the initial boot-up. Therefore, it is recommended to use ONLY HTTP port to access WAF when booting. This displays the status of the unit. *For example, System Booting* . Once the boot process is complete, you are redirected to the login page.


Google Cloud Platform
WAF-Team
Deployment Manager
Deployments
Type registry
bwaf-byol
DELETE
Overview - bwaf-byol
barracuda-web-application-firewall-byol
barracuda-web-application-firewall-byol.jinja
barracuda-web-application-firewall-byol-vm-tmpl vm_instance.py
bwaf-byol-vm vm instance
generated-password-0 password.py
bwaf-byol-tcp-8000 firewall
bwaf-byol-tcp-8443 firewall
barracuda-web-application-firewall-byol
Log into the admin panel
SSH
More about the software

bwaf-byol has been deployed

Barracuda Web Application Firewall (BYOL)
Solution provided by Barracuda Networks, Inc.

Admin URL	http://35.184.27.139:8000/
Admin user	admin
Admin password (Temporary)	iDhXhe3z9p+h
Instance	bwaf-byol-vm
Instance zone	us-central1-f
Instance machine type	n1-standard-1

Get started with Barracuda Web Application Firewall (BYOL)

Suggested next steps

- Request a license
  This is a BYOL solution which requires a valid license to use. Request a license
- Request a license
  This is a BYOL solution which requires a valid license to use. Request a license
- Change the temporary password
  For additional security, it is recommended that you change the password.
- Assign a static external IP address to your VM instance
  An ephemeral external IP address has been assigned to the VM instance. If you require a static external IP address, you may promote the address to static. Learn more

Documentation

Getting Started Guide
How to deploy Barracuda Web Application Firewall in Google Cloud

Product Terms and Conditions
Barracuda Product Terms and Conditions

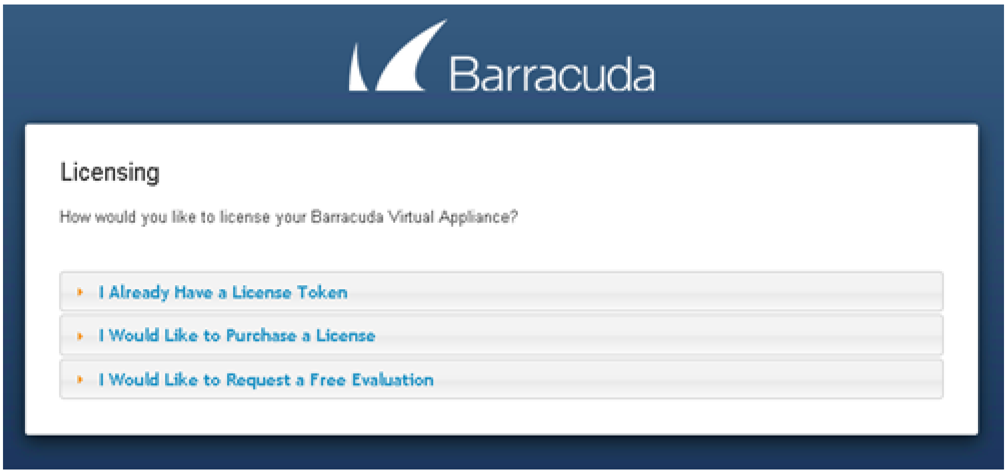
Privacy Policy
Barracuda Privacy Policy

Support

Email and Phone Support offered 24x7 without any phone trees. You will actually

6. After the boot process is complete, the **Licensing** page displays the following options (This step

is skipped in case of PAYG instances)



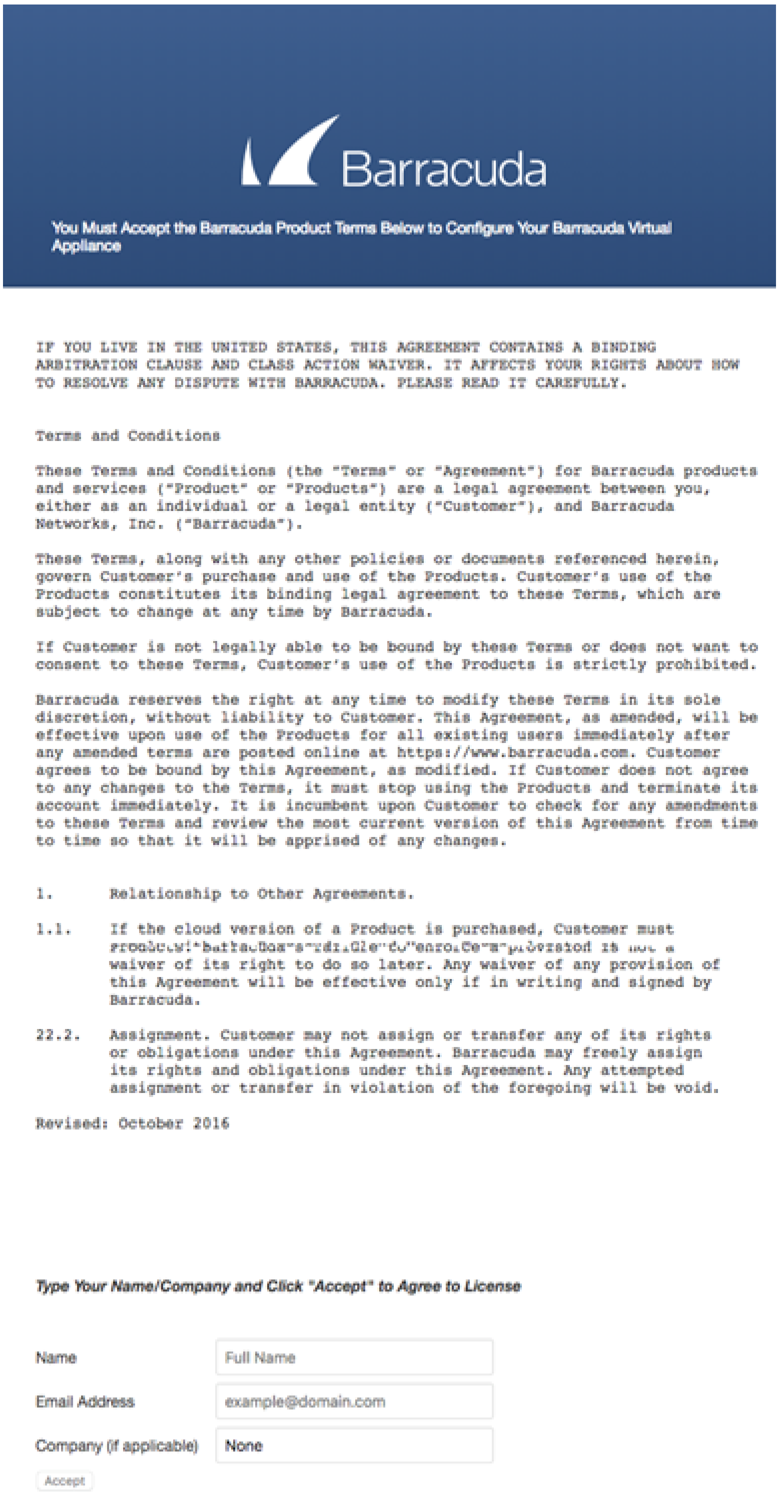
Licensing

How would you like to license your Barracuda Virtual Appliance?

Barracuda
I Already Have a License Token
I Would Like to Purchase a License
I Would Like to Request a Free Evaluation

1. **I Already Have a License Token** – Use this option to provision your Barracuda Web Application Firewall with the license token you have already obtained from Barracuda Networks. Enter your Barracuda Networks **Token** and **Default Domain** to complete licensing, and then click **Provision**.
   The Barracuda Web Application Firewall connects to the Barracuda Update Server to get the required information based on your license and then reboots automatically. Allow a few minutes for the reboot process. Once the instance is provisioned, you are redirected to the login page.
2. **I Would Like to Purchase a License** – Use this option to purchase the license token for the Barracuda Web Application Firewall. Provide the required information in the form, accept the terms and conditions, and click **Purchase**.
   The Barracuda Web Application Firewall connects to the Barracuda Update Server to get the required information based on your license and then reboots automatically. Allow a few minutes for the reboot process. Once the instance is provisioned, you are redirected to the login page.
3. **I Would Like to Request a Free Evaluation** – Use this option to get 30 day free evaluation of the Barracuda Web Application Firewall. Provide the required information in the form, accept the terms and conditions, and click **Evaluate**.
   The Barracuda Web Application Firewall connects to the Barracuda Update Server to get the required information based on your license and then reboots automatically. Allow a few minutes for the reboot process. Once the instance is provisioned, you are redirected to the login page.

After you provide the license key, the Barracuda Web Application Firewall takes some time to be provisioned- typically, within 10 minutes. After the provisioning is complete, fill-in your details to accept the EULA.



You Must Accept the Barracuda Product Terms Below to Configure Your Barracuda Virtual Appliance

IF YOU LIVE IN THE UNITED STATES, THIS AGREEMENT CONTAINS A BINDING ARBITRATION CLAUSE AND CLASS ACTION WAIVER. IT AFFECTS YOUR RIGHTS ABOUT HOW TO RESOLVE ANY DISPUTE WITH BARRACUDA. PLEASE READ IT CAREFULLY.

Terms and Conditions

These Terms and Conditions (the "Terms" or "Agreement") for Barracuda products and services ("Product" or "Products") are a legal agreement between you, either as an individual or a legal entity ("Customer"), and Barracuda Networks, Inc. ("Barracuda").

These Terms, along with any other policies or documents referenced herein, govern Customer's purchase and use of the Products. Customer's use of the Products constitutes its binding legal agreement to these Terms, which are subject to change at any time by Barracuda.

If Customer is not legally able to be bound by these Terms or does not want to consent to these Terms, Customer's use of the Products is strictly prohibited.

Barracuda reserves the right at any time to modify these Terms in its sole discretion, without liability to Customer. This Agreement, as amended, will be effective upon use of the Products for all existing users immediately after any amended terms are posted online at https://www.barracuda.com. Customer agrees to be bound by this Agreement, as modified. If Customer does not agree to any changes to the Terms, it must stop using the Products and terminate its account immediately. It is incumbent upon Customer to check for any amendments to these Terms and review the most current version of this Agreement from time to time so that it will be apprised of any changes.

1. Relationship to Other Agreements.

1.1. If the cloud version of a Product is purchased, Customer must [illegible] is not a waiver of its right to do so later. Any waiver of any provision of this Agreement will be effective only if in writing and signed by Barracuda.

22.2. Assignment. Customer may not assign or transfer any of its rights or obligations under this Agreement. Barracuda may freely assign its rights and obligations under this Agreement. Any attempted assignment or transfer in violation of the foregoing will be void.

Revised: October 2016

Type Your Name/Company and Click "Accept" to Agree to License

Name	Full Name
Email Address	example@domain.com
Company (if applicable)	None

Step 4. Log into Barracuda Web Application Firewall

1. Log into the Barracuda Web Application Firewall using the following credentials.
    1. **Username** – admin

2. **Password** – Use the temporary password displayed on the launch page.

It is recommended to change this password post launch.

1. The **Welcome** screen appears after you log in. If you want to configure your first application, click **Create your first Service**. Otherwise, click **Do it later** if you prefer to familiarize yourself with the user interface. For more information on how to create a Service, refer to Step 6.

Step 5 - Open Network Address Ranges on Firewall

For more information on the list of Open Network Address ranges required for the firewall, refer to the Prepare for the Installation article.

Step 6 - Verify Configuration and Change the Password

1. Either log into the Barracuda Web Application Firewall as an administrator using the Admin URL or click the **Log into the admin panel** button. See **Step 4 - Log into Barracuda Web Application Firewall** for more information.
2. Navigate to the **BASIC > Administration** page and enter your old password, new password, and re-enter the new password.
3. Click **Save Password**.

Step 7 - Configuring the Service(s) on the Barracuda Web Application Firewall

You can configure the services on the **BASIC > Services** page. In Google Cloud Platform, the services can be created using the System (WAN) IP address of the instance.

For more information on services, see Configuring a Service. For adding a service, click the **Help** button.

Figures