Barracuda Web Application Firewall Deployment and Quick Start Guide for Amazon Web Services

https://campus.barracuda.com/doc/41104663/

The Barracuda Web Application Firewall for AWS can be deployed in One-Arm Proxy Mode on Amazon Web Services. This article explains One-Arm Proxy Mode deployment. Complete the steps in this guide to configure, launch, and license your Barracuda Web Application Firewall instance. Then log into the Barracuda Web Application Firewall to verify your configuration and change your password.

Requirements

Before you deploy the Barracuda Web Application Firewall on Amazon Web Services, ensure that you have completed the following:

- Set up an Amazon Virtual Private Cloud (VPC) for the Barracuda Web Application Firewall.
- If you want to use the Bring Your Own Licensing (BYOL) model, get the Barracuda Web Application Firewall license. See Bring Your Own License (BYOL) .

Step 1 - Create a Security Group

Create a security group with rules specifying allowed protocols, ports and source IP ranges. Multiple security groups can be created with different rules, and assigned to each instance. For more information on security groups, refer to the AWS article Amazon EC2 Security Groups.

1. Log into the Amazon EC2 Management Console.
2. From the EC2 dashboard, select **Security Groups** under **Network & Security**.
3. Click **Create security group**.
4. In the **Create security group** window, do the following:
    1. Enter a name to identify the security group.
    2. Specify the description for the security group.
    3. Select a **VPC ID** from the list.
5. Specify the inbound and outbound traffic to be allowed for the instance and click **Create security group**.

By default, the Barracuda Web Application Firewall web interface listens on port 8000 for HTTP and port 8443 for HTTPS. Make sure these ports (8000 and 8443) are allowed by the Inbound rule of the associated security group. Also, add the port(s) through which you configure the Service(s) for this instance.

Step 2 (Optional) - Allocate and Assign an Elastic IP Address to Your Instance

When an instance of your Barracuda Web Application Firewall is created, a public IP address is associated with the instance. That public IP address changes automatically when you **STOP** and **START** the Barracuda Web Application Firewall. To resolve this issue, assign a persistent public IP address to the instance using Elastic IP addressing. For more information, refer to the Amazon Web Services article Elastic IP Addresses.

1. Log into the Amazon EC2 Management Console.
2. From the EC2 dashboard, select **Elastic IPs** under **Network & Security**.
3. Click **Allocate Elastic IP Address.**
4. On the **Allocate Elastic IP address** page, keep the default settings and click **Allocate** to allocate a new IP address. A random Public IP gets generated and displayed in the **Elastic IP addresses** table.
5. In the **Elastic IP addresses** table, click on the new allocated IP address.
6. On the **IP address** page, click **Associate Elastic IP address**.
7. On the **Associate Elastic IP address** page:
    1. Select **Instance** and the **Private IP Address** of the instance from the respective lists. **OR**
    2. Select **Network Interface** and the **Private IP Address** from the respective lists.
    3. Select the **Allow the Elastic IP address to be reassociated** check box.
8. Click **Associate**.

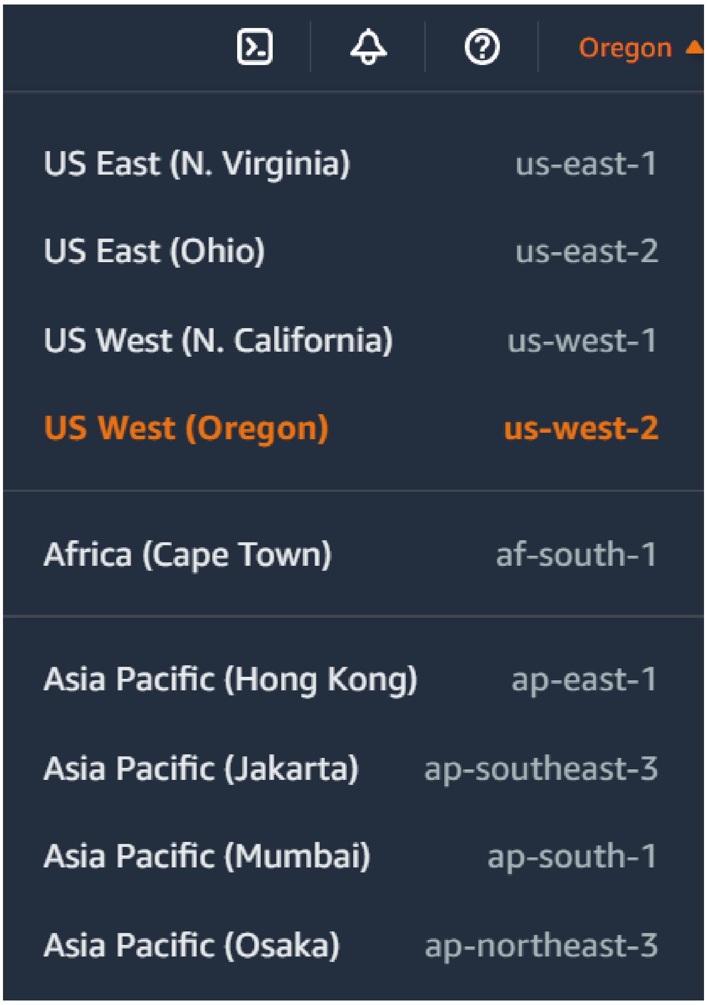
> If you have configured multiple internal IP addresses to the interface, then follow the steps above to allocate and assign the elastic IP address to each internal IP address, so that they can be accessed by the outside world.

Step 3 - Deploy the Barracuda Web Application Firewall on Amazon Web Services

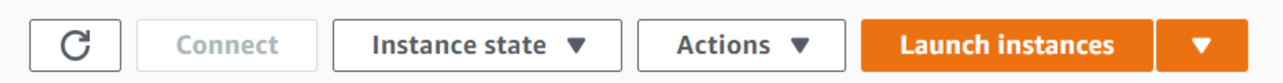
Before you proceed, it is recommended that you go through the Deployment Best Practices article.

In the Amazon VPC that you configured, launch an Amazon EC2 instance with the Barracuda Web Application Firewall AMI image. The **Amazon Launch Instance** wizard guides you through the following steps:

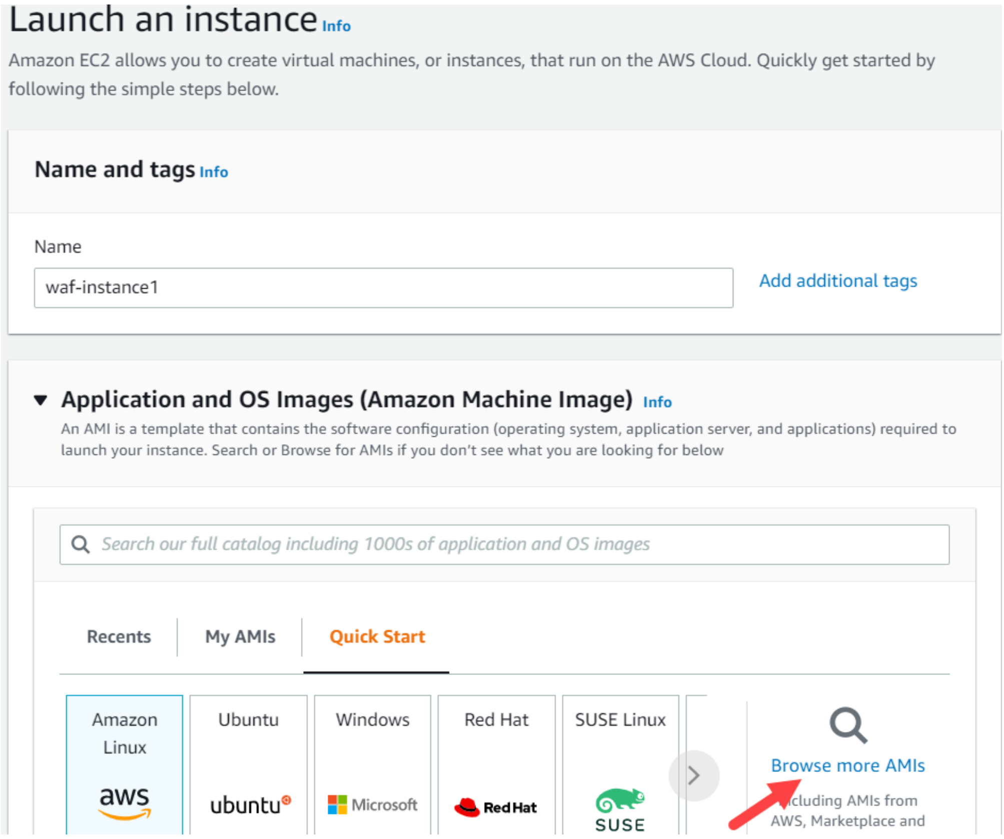
1. Log into the AWS Management Console and open the EC2 Management Console.
2. From the top right corner of the page, select the region for the instance. This is important because some Amazon EC2 resources can be shared between regions.


Oregon
US East (N. Virginia) us-east-1
US East (Ohio) us-east-2
US West (N. California) us-west-1
US West (Oregon) us-west-2
Africa (Cape Town) af-south-1
Asia Pacific (Hong Kong) ap-east-1
Asia Pacific (Jakarta) ap-southeast-3
Asia Pacific (Mumbai) ap-south-1
Asia Pacific (Osaka) ap-northeast-3

3. Select **Instances** under **Instances**.
4. On the **Instances** page, click **Launch Instances**.



5. On the **Launch an instance** page, do the following:
    1. **Name and tags**
        1. **Name**: Specify a name for the instance.
    2. **Application and OS Images (Amazon Machine Image)**
        1. Click **Browse more AMIs**.



Launch an instance Info

Amazon EC2 allows you to create virtual machines, or instances, that run on the AWS Cloud. Quickly get started by following the simple steps below.

Name and tags Info

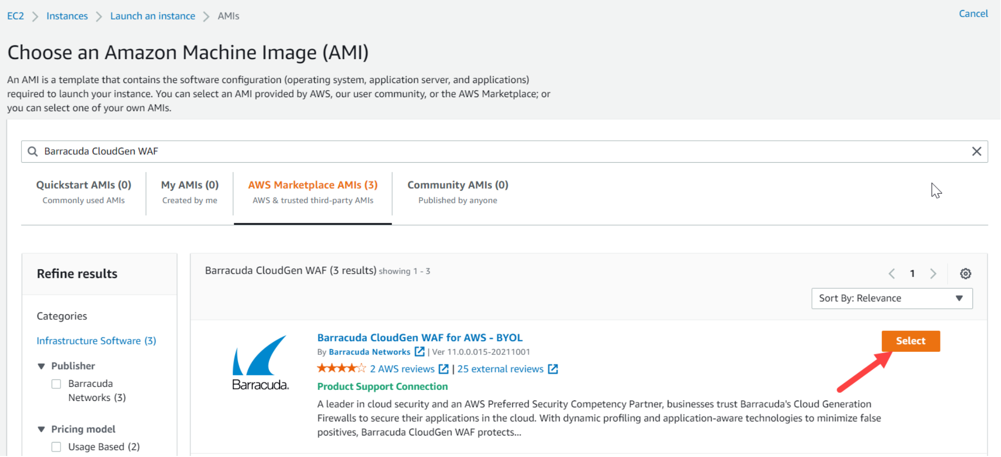
Name: waf-instance1

Application and OS Images (Amazon Machine Image) Info

An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. Search or Browse for AMIs if you don't see what you are looking for below

Add additional tags
Search our full catalog including 1000s of application and OS images
Recents
My AMIs
Quick Start
Amazon Linux
Ubuntu
Windows
Red Hat
SUSE Linux
Browse more AMIs
Including AMIs from AWS, Marketplace and

2. On the **Choose an Amazon Machine Image (AMI)** page:
    1. Select **AWS Marketplace AMIs** and search for the *Barracuda Web Application Firewall* AMI. Click **Select** next to the Barracuda Web Application Firewall AMI.



Choose an Amazon Machine Image (AMI)

An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. You can select an AMI provided by AWS, our user community, or the AWS Marketplace; or you can select one of your own AMIs.

Search: Barracuda CloudGen WAF

Barracuda CloudGen WAF (3 results) showing 1 - 3

Barracuda CloudGen WAF for AWS - BYOL

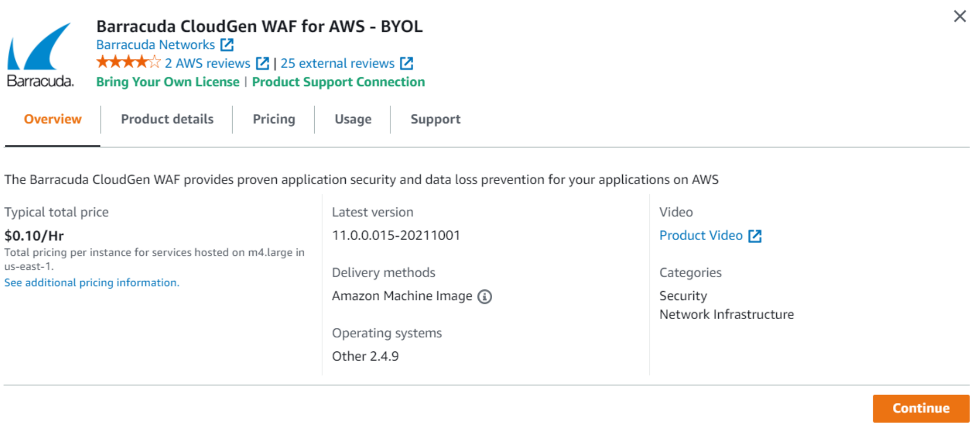
By Barracuda Networks | Ver 11.0.0.015-20211001

2 AWS reviews | 25 external reviews

Product Support Connection

A leader in cloud security and an AWS Preferred Security Competency Partner, businesses trust Barracuda's Cloud Generation Firewalls to secure their applications in the cloud. With dynamic profiling and application-aware technologies to minimize false positives, Barracuda CloudGen WAF protects...

    2. Go through the overview and product details and click **Continue**.



Barracuda CloudGen WAF for AWS - BYOL

Barracuda Networks

★★★★☆ 2 AWS reviews | 25 external reviews

Bring Your Own License | Product Support Connection

The Barracuda CloudGen WAF provides proven application security and data loss prevention for your applications on AWS

Typical total price

$0.10/Hr

Total pricing per instance for services hosted on m4.large in us-east-1.

See additional pricing information.

Latest version

11.0.0.015-20211001

Delivery methods

Amazon Machine Image

Operating systems

Other 2.4.9

Video

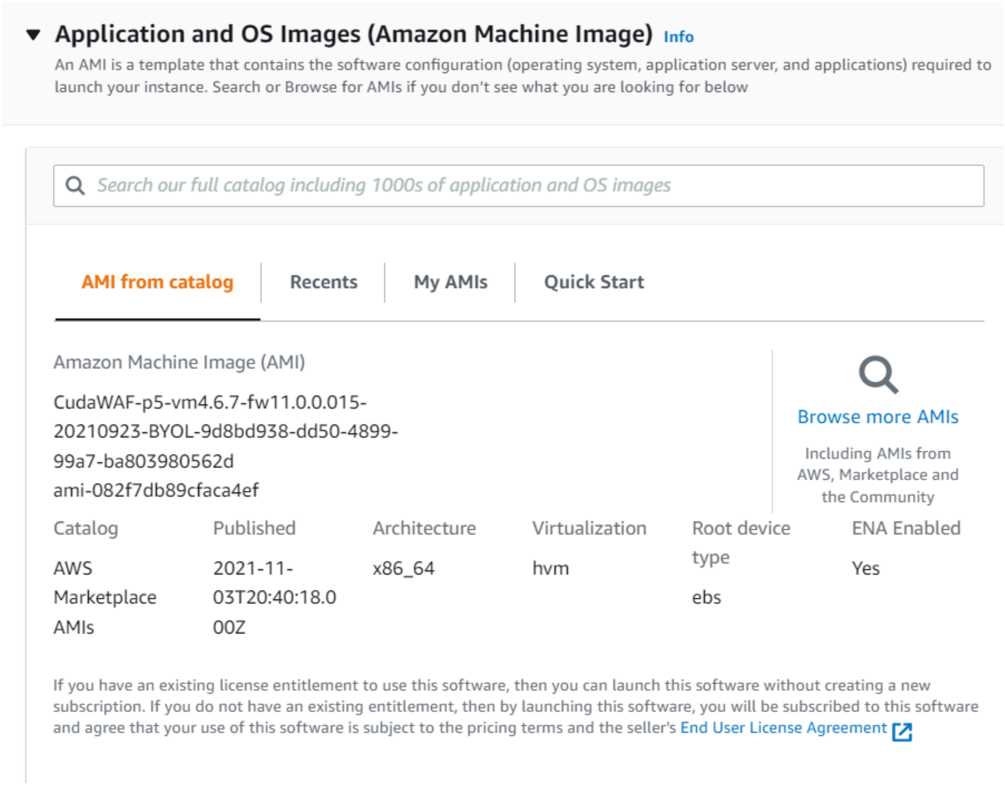
Product Video

Categories

Security
Network Infrastructure

3. Click **Confirm Changes** when prompted.

3. The selected AMI appears on the **Launch an instance** page.



▼ **Application and OS Images (Amazon Machine Image)** Info

An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. Search or Browse for AMIs if you don't see what you are looking for below

Search our full catalog including 1000s of application and OS images

Amazon Machine Image (AMI)

CudaWAF-p5-vm4.6.7-fw11.0.0.015-20210923-BYOL-9d8bd938-dd50-4899-99a7-ba803980562d
ami-082f7db89cfaca4ef

Browse more AMIs

Including AMIs from AWS, Marketplace and the Community

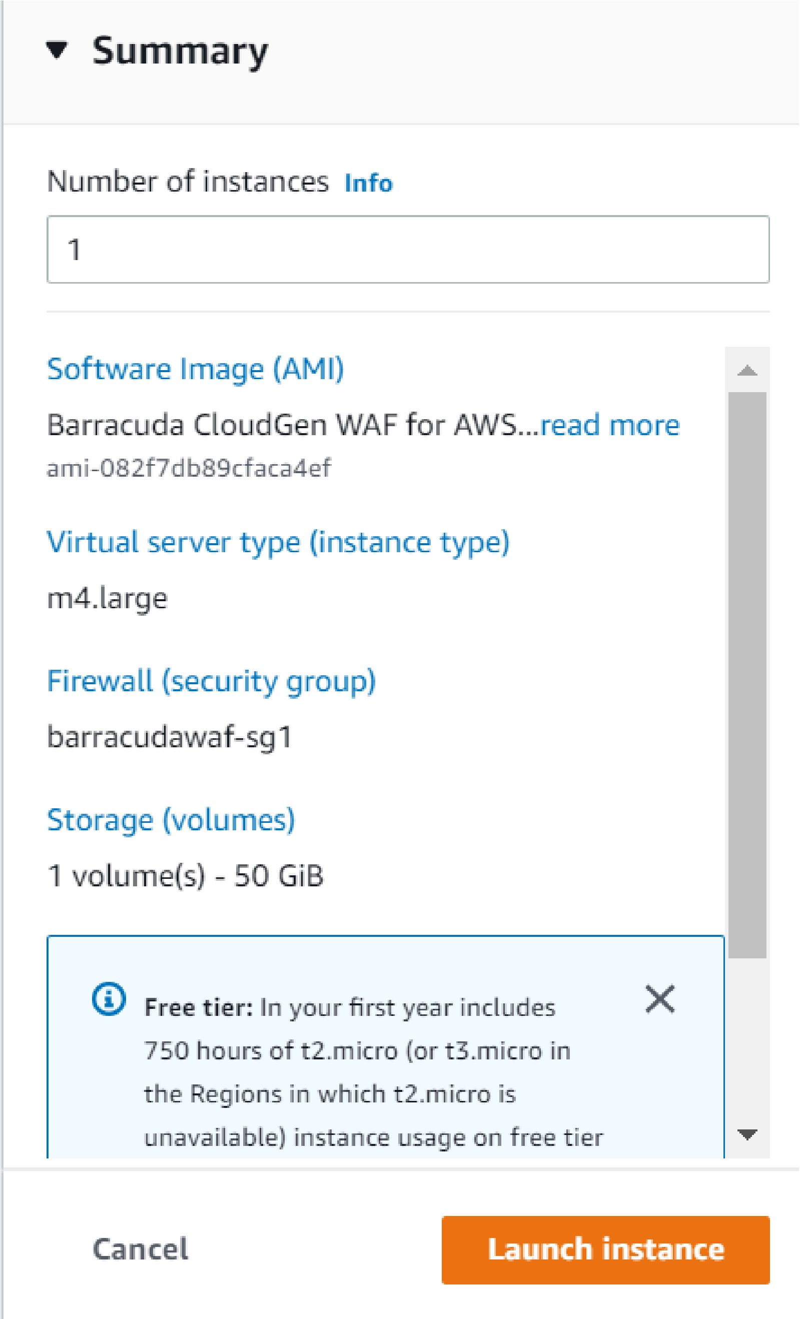
Catalog	Published	Architecture	Virtualization	Root device type	ENA Enabled
AWS Marketplace AMIs	2021-11-03T20:40:18.000Z	x86_64	hvm	ebs	Yes

If you have an existing license entitlement to use this software, then you can launch this software without creating a new subscription. If you do not have an existing entitlement, then by launching this software, you will be subscribed to this software and agree that your use of this software is subject to the pricing terms and the seller's End User License Agreement

3. **Instance type**
   1. Select an instance type from the drop-down list.
4. **Key pair (login)**
   1. Select the existing key pair or create a new key pair.
5. **Network Settings**
   1. **VPC**: Select the VPC from the drop-down list.
   2. **Subnet**: Select a subnet from the drop-down list. Make sure to select the subnet of the VPC where you want to create the instance.
   3. **Firewall (security groups)**: Click **Select existing security group** to select and assign the security group(s) from the existing list, or choose **Create security group** to create a new group.

6. **Configure Storage**
    1. The storage device settings for the instance is displayed. Modify the values if required.
7. **Advanced details**
    1. Keep the default setting for all parameters.

6. Review your settings under **Summary** and click **Launch instance**.



▼ Summary

Number of instances Info

1

Software Image (AMI)

Barracuda CloudGen WAF for AWS...read more

ami-082f7db89cfaca4ef

Virtual server type (instance type)

m4.large

Firewall (security group)

barracudawaf-sg1

Storage (volumes)

1 volume(s) - 50 GiB

Free tier: In your first year includes 750 hours of t2.micro (or t3.micro in the Regions in which t2.micro is unavailable) instance usage on free tier

After you click **Launch instance**, Amazon Web Services begins provisioning the Barracuda Web Application Firewall. Allow a few minutes for the Amazon Web Services Agent and the Barracuda Web Application Firewall image to boot up.

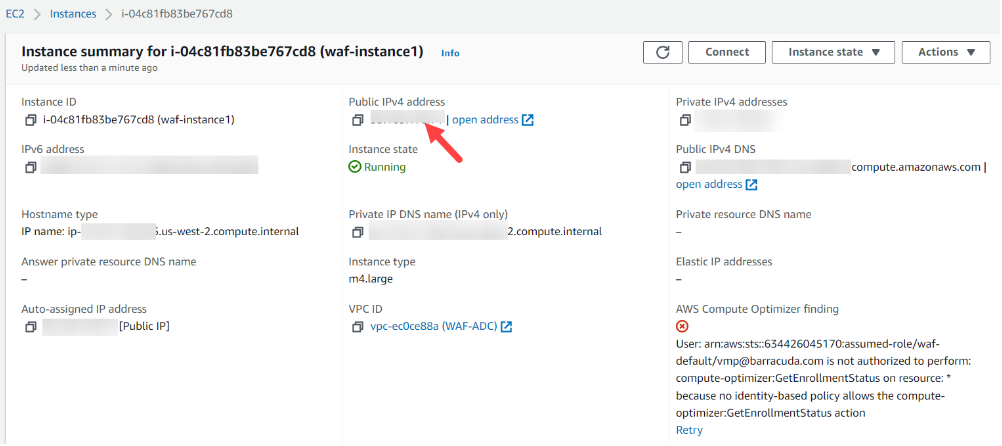
DO NOT restart the Barracuda Web Application Firewall while it is launching!

Step 4 - License the Barracuda Web Application Firewall

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

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

1. Log into the Amazon EC2 Management Console.
2. From the EC2 Dashboard, select **Instances** under **Instances**.
3. In the **Instances** table, select the Barracuda Web Application Firewall instance you created and note the **Public IPv4 address**.



Instance summary for i-04c81fb83be767cd8 (waf-instance1)
Updated less than a minute ago

Instance ID
i-04c81fb83be767cd8 (waf-instance1)

IPv6 address
[redacted]

Hostname type
IP name: ip-[redacted].us-west-2.compute.internal

Answer private resource DNS name
–

Auto-assigned IP address
[redacted] [Public IP]

Public IPv4 address
[redacted] | open address

Instance state
Running

Private IP DNS name (IPv4 only)
[redacted]2.compute.internal

Instance type
m4.large

VPC ID
vpc-ec0ce88a (WAF-ADC)

Private IPv4 addresses
[redacted]

Public IPv4 DNS
[redacted]compute.amazonaws.com | open address

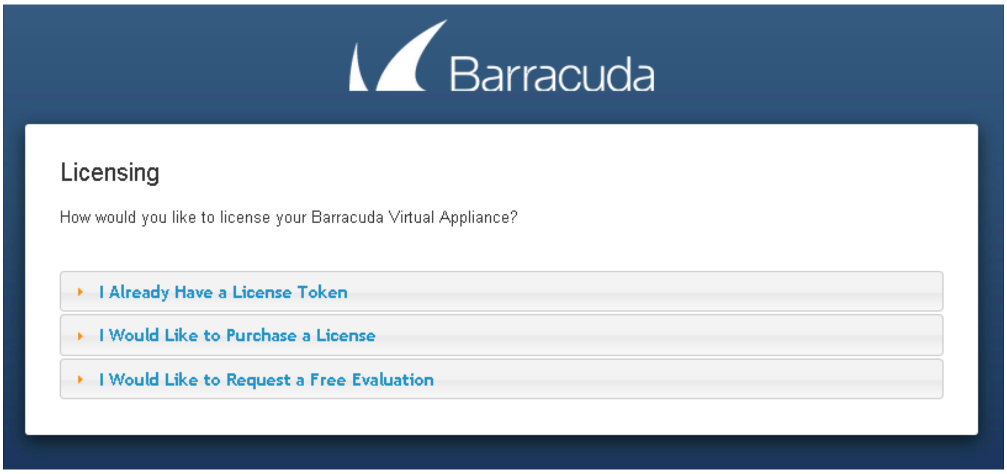
Private resource DNS name
–

Elastic IP addresses
–

AWS Compute Optimizer finding
User: arn:aws:sts::634426045170:assumed-role/waf-default/vmp@barracuda.com is not authorized to perform: compute-optimizer:GetEnrollmentStatus on resource: * because no identity-based policy allows the compute-optimizer:GetEnrollmentStatus action
Retry

4. Open the browser and enter the copied Elastic IP address (from step **3**) with port 8000 for HTTP. No port is required for HTTPS. For example:
   For HTTP: http://<Public DNS>:8000 (Unsecured)
   For HTTPS: https://<Public DNS> (Secured)

   The Barracuda Web Application Firewall is not accessible via HTTPS port when it is booting up. Therefore, use ONLY HTTP port to access the unit when booting. This displays the status of the unit i.e., System Booting. Once the boot process is complete, you will be redirected to the login page.
5. After the boot process is complete, the **Licensing** page displays with the following options:



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 days 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.

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. Log into the Barracuda Web Application Firewall web interface as the administrator using the URL, as described in step 4 of **Licensing of the Barracuda Web Application Firewall after deploying on Amazon Web Services** above. Log in with:
    1. **Username*:*** *admin*
    2. **Password**: **Instance ID** of your Barracuda Web Application Firewall in Amazon Web Services.
2. Navigate to the **BASIC > Administration** page and enter your old password, new password, and re-enter the new password. Click **Save Password**.

Configuring the Service(s) on the Barracuda Web Application Firewall

You can configure the services on the **BASIC > Services** page. In Amazon Web Services, the services can be created either using the System (WAN) IP address of the instance or any other IP address from the IP address pool as your System (WAN) IP address in the **Virtual IP Address** field. Note that configuring the VIP with an IP address from the IP address pool as your System (WAN) IP address is possible only for stand-alone instances. Also, ensure that you:

- Assign multiple private IP addresses to the network interface of the deployed Barracuda Web Application Firewall instance. The assigned private IP addresses can be used to create the service(s) on the Barracuda Web Application Firewall. For information on how to assign multiple private IP addresses, see Step 3 - (Optional) Assign Multiple Private IP Addresses to the Network Interface of the Instance.
- Allocate and assign an Elastic IP (EIP) address to each private IP address assigned to the network interface of the Barracuda Web Application Firewall instance, so that it can be accessed externally. Ensure that the corresponding ports are opened in your security group and firewall. For more information on how to assign the EIP to the private IP address, see Step 4 - Allocate and Assign an Elastic IP Address to your Instance.

If you want to cluster the Barracuda Web Application Firewall instances to load balance the traffic, ensure that the services are created using only the System (WAN) IP address. After the service is created using the System (WAN) IP address, the service will be accessible through the Public IP/DNS of the Barracuda Web Application Firewall VM. Ensure that the corresponding ports are opened in your security group and firewall.

For more information on services, see Step 2: Configuring a Service. For detailed instructions on how to add a service, click the **Help** button.

Figures