Configuring Multiple IP Addresses for the Barracuda Web Application Firewall Instance in Amazon Web Services

https://campus.barracuda.com/doc/90446629/

You can deploy the Barracuda Web Application Firewall instance(s) with **Single NIC** and **Multi IP** on Amazon Web Services. This article provides information on how to configure services with multiple IP addresses in the Barracuda Web Application Firewall.

Prerequisites

- Create an IAM role. You can refer to the following link for more information on how to create and manage an IAM policy.
  Below is the policy attachment required by an IAM role for making the AWS multi-IP work:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeNetworkInterfaces",
                "ec2:UnassignPrivateIpAddresses",
                "ec2:AssignPrivateIpAddresses"
            ],
            "Resource": "*"
        }
    ]
}
```

Perform the following steps to enable and use multiple IP feature in the Barracuda Web Application Firewall:

1. Enable Multi IP Configuration for Services.
2. Create the Service(s) Using the Multi IP Addresses.

Enable Multi IP Configuration for Services

After deploying the Barracuda Web Application Firewall instance with single NIC, continue with "Step 2. Licensing the Barracuda Web Application Firewall on Amazon Web Services" in the Barracuda Web

Application Firewall Deployment and Quick Start Guide for Amazon Web Services

To enable multiple IP feature on the Barracuda Web Application Firewall, perform the following steps:

1. Log into the Barracuda Web Application Firewall web interface.
2. Go to the **BASIC > IP Configuration** page, set **Enable Multi IP Configuration** to **Yes**
3. Click **Save**.

Create the Service(s) Using the Multiple IP Addresses

After enabling **Multi IP** in the **BASIC > IP Configuration** page, you can create services with different IP addresses. When **Multi IP Enable** is set to **Yes**, you can create a service by the following methods:

- Using an existing service IP address with a different port number.
- Using the IP address that belongs to the configured subnet on Amazon Web Services.
- Using the IP address that is already configured on the Amazon Web Services interface.
- Allowing Amazon Web Services to allocate a new IP address.

For detailed instructions on configuring a service, go to the **BASIC > Services** page and click **Help**.

Below is the example to create an HTTP service:

1. Go to the **BASIC > Services** page.
2. In the **Add New Service** section, specify values for the following:
    - **Service Name** - Enter a name for the service.
    - **Type** - Select **HTTP**. For more information on service types, see Services.
    - **Virtual IP Address** - Assign the IP address to the service either by using the IP address that belongs to the configured subnet on Amazon Web Services, or by allowing Amazon Web Services to allocate a new IP address.
        - To manually enter the IP address, select **Enter IP Address** and specify the IP address in the text field.
        - To allow Amazon Web Services to allocate a new IP address, select **Allocate New IP**.
        - Also, you can create a new service using the existing service IP address with a different port.
    - **Port** - Enter the port number on which the web server responds.
    - **Real Servers** - Enter the IP address of the server that hosts the service. This is the backend server that is protected by the Barracuda Web Application Firewall.
    - **Service Groups** – Select the group under which the service needs to be added.
3. Click **Add**.

How Multi IP Address Works in Stand-Alone System

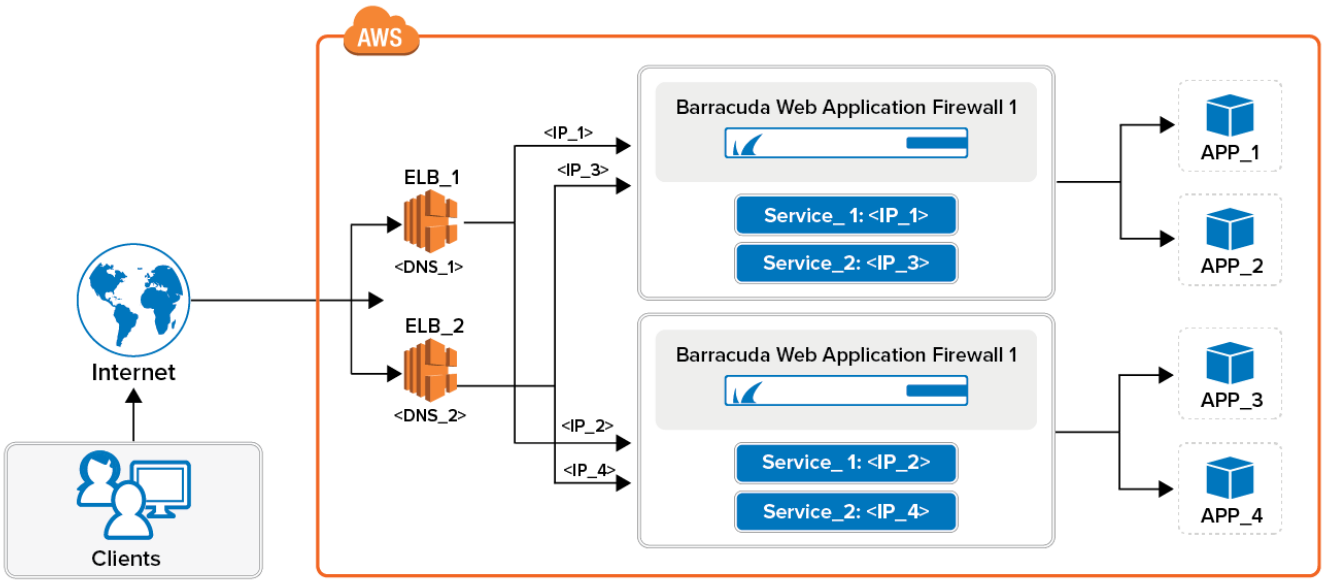
If a service is created using an IP address other than the existing service IP address, the private IP address gets added automatically under the WAN interface of the instance on the Amazon Web Services portal. The private IP address should be assigned with a load balancer for the service to be accessible from the external network (internet). For example, if service_1 (10.83.1.5) and service_2 (10.83.1.6) are created using port 80, the IP addresses should be assigned to the load balancer(which assigns a DNS name) on Amazon Web Services. In this example, service_1 (10.83.1.5) is mapped with ELB_1 and service_2 (10.83.1.6) is mapped with the ELB_2.

Now, the users can access both the services (service_1 and service_2) using the same port 80 via two different DNS Servers so that the applications can be accessed using the DNS names. For example, if service_1 (10.83.1.5) is mapped to ELB_1 and service_2 (10.83.1.6) is resolved toELB_2, the applications can be accessed using the DNS names (abc.com and xyz.com respectively).

How Multi IP Address Works in Clustered Systems

If a service is created using the IP address other than the existing service IP address, the private IP address gets added automatically under the WAN interface of the instance on the Amazon Web Services portal. The private IP address should be assigned with a load balancer for the service to be accessible from the external network (internet).

If the Barracuda Web Application Firewall instances are in a cluster, the following should be manually configured in the load balancer to which the instances are associated with:



Load Balancing

This section describes load balancing across multiple services with the AWS ELB (Application Load Balancer). Create an AWS ELB (Application Load Balancer) for each application configured on the Barracuda Web Application Firewall.

For more information on how to create an ELB on AWS, see https://docs.aws.amazon.com/elasticloadbalancing/latest/application/create-application-load-balancer.html

While creating the ELB, ensure that you choose the target group as an "IP Address". Multiple IP addresses can be added later to this target group and AWS ELB can load balance across these multiple IP addresses.

Configure the load balancing rule to distribute the traffic to the services specified in the back-end pool across the clustered instances. For example, requests to Service_1 are distributed between WAF_1 and WAF_2.

In this section, the load balancer configuration is explained with an example. Consider*WAF_1* and *WAF_2* are the two instances that are in a cluster. *WAF_1* is configured with Service_1: IP_1 and Service_2: IP_3 and the same services are displayed with different IP addresses in *WAF_2* i.e. Service_1: IP_2 and Service_2: IP_4. The Public DNS assigned to Service_1 and Service_2 are DNS_1 and DNS_2 respectively. DNS_1 and DNS_2 are the load balancer DNS names that are represented as

xxxxxxxx.us-west-2.elb.amazonaws.com

Multi-IP Refresh

When a Multi IP backup restore is performed, the old IPs get restored on the new instance. To refresh these IPs, the user can now perform a bulk refresh of all the multi IPs configured on the Barracuda Web Application Firewall.

To refresh Multi IPs:

1. In the **More Actions** drop-down list, select **Multi IPs Refresh**.
2. In the **Multi IPs Refresh** window:
    1. Select the object type (service, server, or rule group) that needs to be refreshed.
    2. Select the service that needs to be refreshed, and from the drop-down list, choose between **Allocate New IP** or **Enter IP Address** for a refresh. You can either allocate a new IP to the service or enter the existing IP address that needs a refresh.
3. Click **Save**.

The feature is available for all cloud instances that support Multi IP. However, this is currently visible only on non-clustered units. Also, note that the units that are in HA do not have this option.

Figures