The **Barracuda CloudGen WAF** for AWS solution is found in the AWS Marketplace and offers the following key benefits:

- Dynamic profiling and application-aware technology that helps minimize false-positives
- Out of the box configurations and rule sets that drive rapid deployment for complex requirements.
- Data loss protection
- Automated detection and blocking of application attacks, like SQL Injection, XSS, Malware uploads, and application DDoS attacks.
- Built-in access controls that enable administrators to create granular policies for Authentication, Authorization, & Accounting
- An Integrated Barracuda Vulnerability Remediation Service that removes much of the administrative overhead traditionally associated with firewall maintenance by enabling automatic configuration of security policies.
Before using the Barracuda CloudGen WAF for AWS Solution, you will need to set up a VPC (virtual private cloud) using the steps below. If you already have a VPC set up, then you can skip these steps.

Part 1: Setting up a VPC

Step 1 Log into your AWS Dashboard.

Step 2 Navigate to your VPC dashboard by selecting VPC under the Networking & Content Delivery section.

Step 3 Next, click the Launch VPC Wizard button at the top-left.

Step 4 At the next screen, select the type of VPC that you want to set up by clicking on it and choosing the blue-colored Select button.
**Step 5**  
Next, enter a name for your VPC and customize the IP address information. You will also see an option to add an IPv6 CIDR block.

**Step 6**  
Once you have named and configured your VPC, select the Create VPC button at the bottom-right to create it.
Once you have set up a VPC, you will then be able to set up and configure the Barracuda CloudGen WAF for AWS solution.

**Part 2: Set up and Configuration of the Barracuda CloudGen WAF for AWS solution**

**Step 1**  
Locate the Barracuda CloudGen WAF for AWS solution in the AWS Marketplace and select the Continue to Subscribe button, if not already subscribed.

**Step 2**  
Select the Continue to Configuration button.
Step 3

Next, you will see an option to choose the AMI (Amazon Machine Image), software version, and region you would like to use. Then, click the Continue to Launch button.

![Image of AMI selection screen]

Step 4

At the next screen, you will be able to select an Action to either launch the Barracuda CloudGen WAF for AWS solution through an EC2 Instance or to Copy to the Service Catalog. Select the option to Launch through EC2.

![Image of action selection screen]

Part 2 of 3

Steps 5 of 7
Step 5

Once you launch the EC2 instance, you will be taken to a login page for the Barracuda CloudGen WAF for AWS solution.

The initial login credentials for this page will be:
Username: admin
The password will be the EC2 instance ID number. You can find the EC2 instance ID number under your running EC2 instances in the AWS Dashboard.
Example: i-56146er654erghe
Step 6  After you log in, you will be taken to the main dashboard page for the Barracuda CloudGen WAF for AWS solution.

Step 7  Navigate through all items under the Basic, Security Policies, Websites, Access Control, Networks, and Advanced main tabs and complete the all configuration items that are pertinent to your organization.
Part 3: The Integrated Barracuda Vulnerability Remediation Service

Note: The Barracuda Vulnerability Remediation Service is integrated in the Barracuda CloudGen WAF for AWS solution. The demonstration video shows a scan using this service against a demo web application.

Step 1  Click the **web application** button at the top-right of the page.

Step 2  Next, enter in the information of your Web application or select the “Click Here” option on the right-side of the pop-up window to use the Demo Web Application for the scan.
Step 3  Next, select the **Run Now** option at the bottom-right to run a manual scan. 
Note: The scan may take up to 30-60 minutes to complete.

Step 4  Next, click the **Scan Status** option at the top left of the page and select the See Finish Scan option below the scan results.
Step 5  
Next, under the Report area on the far right, select either the View or Download options. For this example, we will use the **View** option.

![Vulnerability Scan Results](image1)

Step 6  
You will now see the results of the vulnerability scan.

![Vulnerability Remediation Service](image2)

Complete
Thank you.

For more information, visit https://amzn.to/2MBEz8g