How to Deploy a Volume-Based (Metered) PAYG CloudGen Firewall Image in AWS

https://campus.barracuda.com/doc/79463334/

When deploying a PAYG CloudGen Firewall in AWS, you can pay for your firewall licenses per hour or per amount of traffic handled by the firewall. The volume-based PAYG CloudGen Firewall image is deployed just like the other CloudGen Firewall images in the AWS Marketplace, with one additional IAM policy to allow the firewall to report the data usage to the AWS Marketplace. Failing to include the required IAM role policies causes the firewall license to switch to Grace Expired mode. To safeguard against unexpected high traffic usage, Barracuda Networks recommends to configure CloudWatch alarms to monitor traffic passing through the firewall.

For more information on volume-based PAYG licensing, see Public Cloud Licensing.



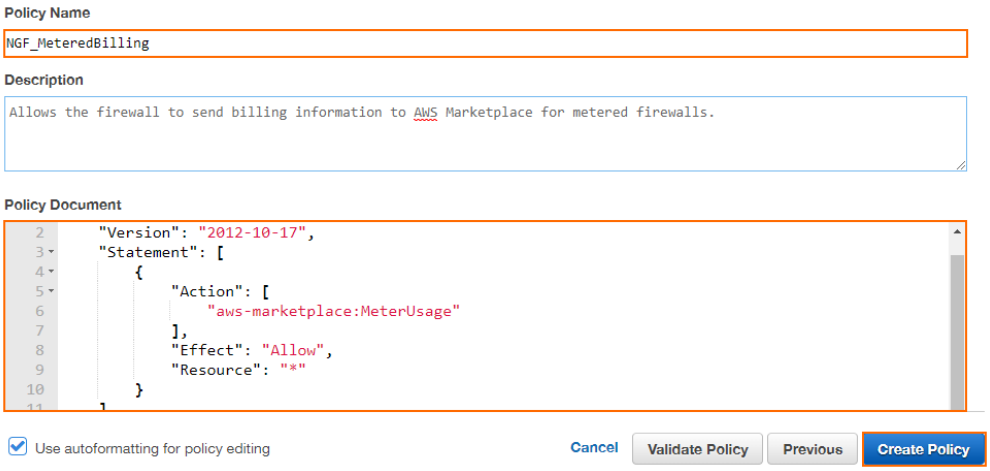
Before You Begin

(optional) Identify the AWS reference architecture and download the template you want to deploy. For more information, see Implementation Guide - CloudGen Firewall in AWS.

Step 1. Create an IAM Role for the Firewall

Create an IAM role for your firewall instance. Verify that all the IAM policies required for the selected reference architecture are included in the IAM role. The following IAM policies are required:

- AWS Marketplace Metered Billing
- AWS CloudWatch



For step-by-step instructions, see How to Create an IAM Role for a CloudGen Firewall in AWS.

Step 2. Deploy the Firewall

Deploy the CloudGen Firewall via AWS Console or CloudFormation template. For template deployments, verify that the correct volume-based PAYG firewall IAM is used for your region.

- **AWS console** – For more information, see How to Deploy a CloudGen Firewall in AWS via AWS Console.
- **CloudFormation Templates** – For more information, see How to Deploy a CloudGen in AWS via CloudFormation Template.
- **AWS Reference Architectures** – For more information, see Implementation Guide - CloudGen Firewall in AWS.

Your CloudGen Firewall is now reporting the traffic metrics every full hour to the AWS Marketplace.

Next Steps

Configure CloudWatch alarms to monitor traffic to and from the firewall to safeguard against unexpected high traffic usage.

Figures

1. aws_report_traffic.png
2. aws_IAM_role_12.png

© Barracuda Networks Inc., 2024 The information contained within this document is confidential and proprietary to Barracuda Networks Inc. No portion of this document may be copied, distributed, publicized or used for other than internal documentary purposes without the written consent of an official representative of Barracuda Networks Inc. All specifications are subject to change without notice. Barracuda Networks Inc. assumes no responsibility for any inaccuracies in this document. Barracuda Networks Inc. reserves the right to change, modify, transfer, or otherwise revise this publication without notice.