How to Deploy a CloudGen Firewall Auto Scaling Cluster in AWS

https://campus.barracuda.com/doc/79463333/

A CloudGen Firewall Auto Scaling cluster automatically scales with demand, thereby creating a cost-effective, robust solution for securing and connecting to your cloud resources. The firewall cluster integrates tightly with AWS services and APIs. Configuration changes are synchronized securely over the AWS backend, with all instances sharing the same configuration. For the admin, the firewall cluster handles like a single CloudGen Firewall. The firewall cluster uses the PAYG image of the Barracuda CloudGen Firewall in the AWS Marketplace to allow you to quickly deploy without the need for long-term licensing commitments. CloudGen Firewall clusters cannot be managed by a Control Center. The following custom metrics are collected from the firewall cluster:

All custom metrics are published in to the **Barracuda/NGF** namespace.

Custom VPN Metrics

- Client to Site VPN tunnels
- SSL VPN clients
- Site to Site VPN tunnels up
- Site to Site VPN tunnels down

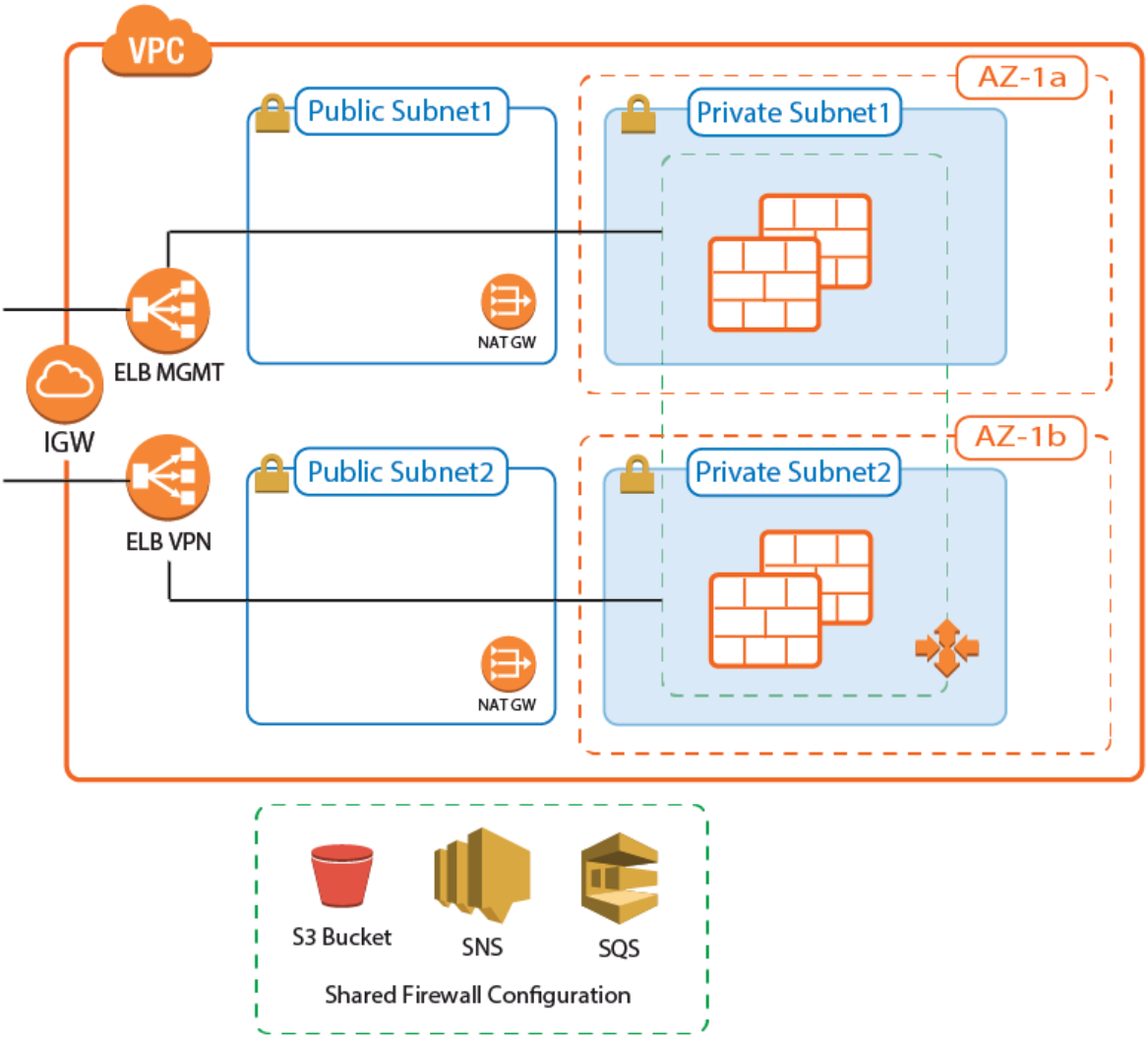
Custom System Metrics

- load
- Used memory
- Protected IPs

Custom Firewall Metrics

- Forwarding Firewall Sessions bps
- Forwarding Firewall Sessions packets
- Bytes in
- Bytes out
- Bytes total
- Packets in
- Packets out
- Packets total
- Connections dropped
- IPS Hits
- Forwarding Connections new
- Forwarding Connections total
- Connections new
- Connections total
- Connections blocked

- Connections failed



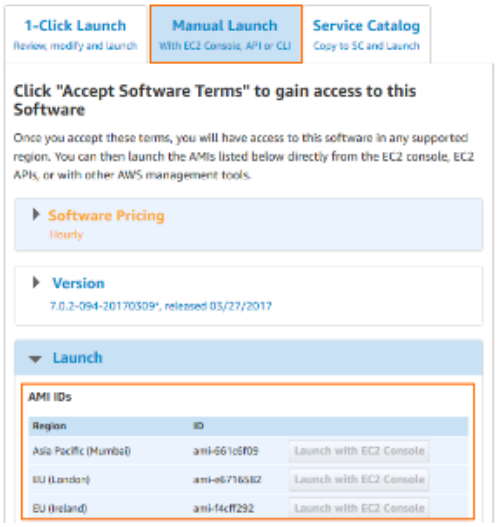
AWS Reference Architectures

This article is used in the following AWS reference architectures:

- AWS Reference Architecture - CloudGen Firewall Auto Scaling Cluster
- AWS Reference Architecture - CloudGen Firewall Cold Standby Cluster

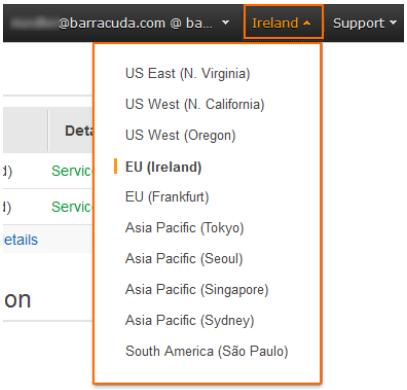
Before You Begin

- Download the template from the Barracuda Network GitHub account: https://github.com/barracudanetworks/ngf-aws-templates.
  - **CloudGen Firewall Auto Scaling Cluster** – Download **autoscale.json**
  - **CloudGen Firewall Cold Standby Cluster** – Download **coldstandby.json**
- Verify that the AMI image IDs used in the CloudFormation template match the IDs for the CloudGen Firewall image listed in the AWS Marketplace. The AMI disk images change for every released version and differ for each region.



Step 1. Select the AWS Datacenter

1. Log into the AWS console.
2. In the upper right, click the datacenter location, and select the datacenter you want to deploy to from the list.



The selected datacenter location is now displayed in the AWS console.

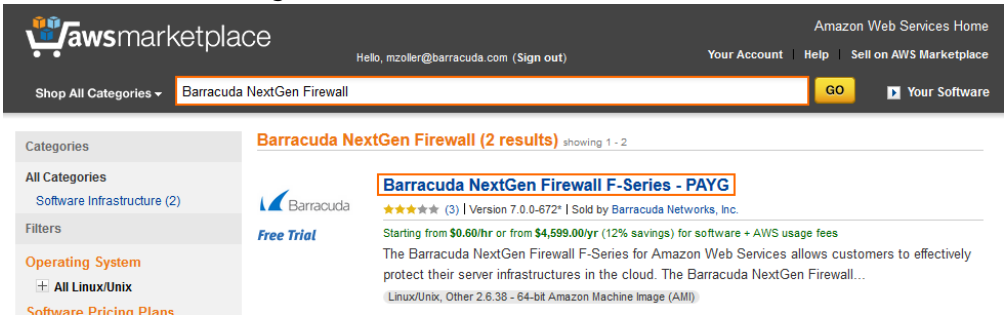
Step 2. Create an IAM Role for the Firewall

Create an IAM Role to allow the firewall instances to make the required API calls.
For more information, see How to Create an IAM Role for a CloudGen Firewall in AWS.

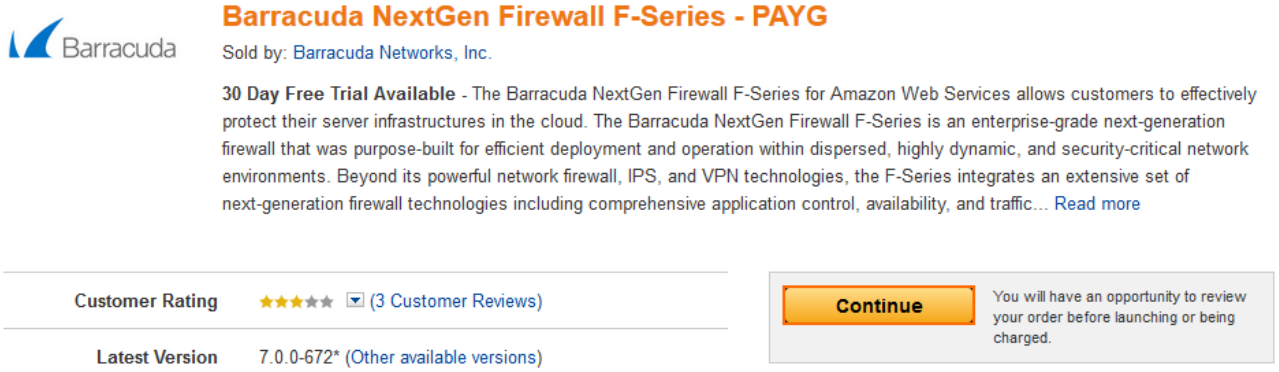
Step 3. Subscribe to Barracuda CloudGen Firewall F-Series PAYG AMI in AWS Marketplace

To be able to deploy a CloudGen Firewall PAYG image via the CloudFormation template, you must agree to the **Terms of Service** and subscribe to the image in the AWS Marketplace. You need to do this only once per account,

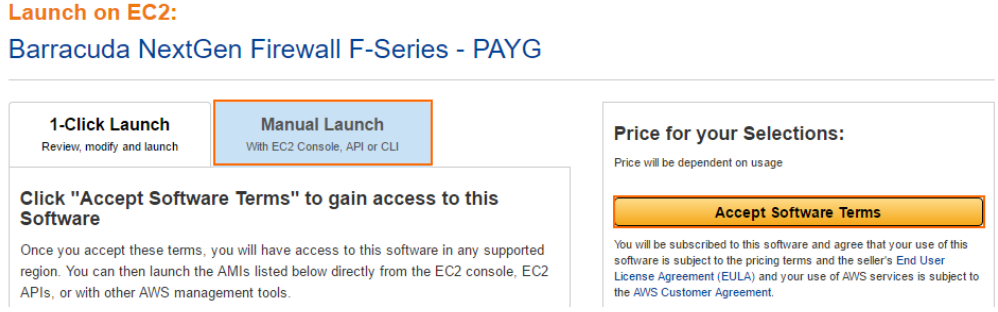
1. Go to the AWS Marketplace: https://aws.amazon.com/marketplace/
2. Search for `Barracuda CloudGen Firewall` .
3. Click the **Barracuda CloudGen Firewall F-Series PAYG** or **Barracuda CloudGen Firewall F-Series BYOL** image.



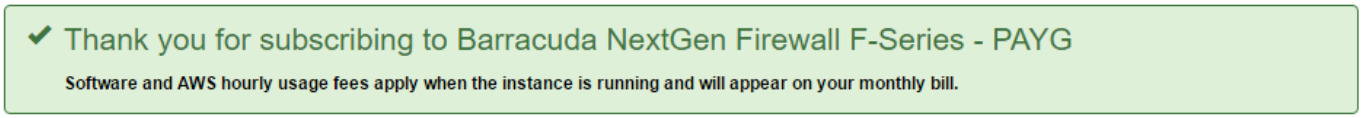
4. Click **Continue**.



5. Click the **Manual Launch** tab.
6. Click **Accept Software Terms**.



You will now receive an email from Amazon confirming your subscription. You can now use the provided AMI in your CloudFormation templates.

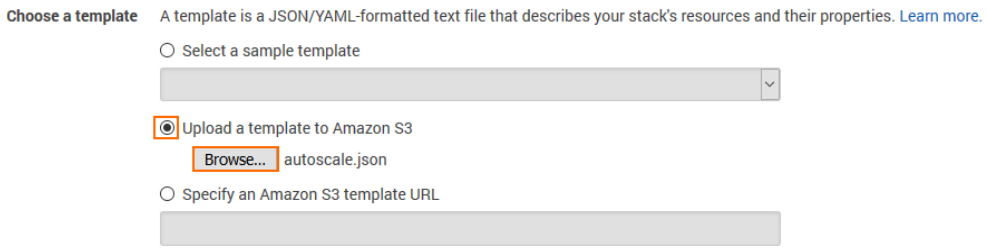


Step 3. Deploy the CloudFormation Template

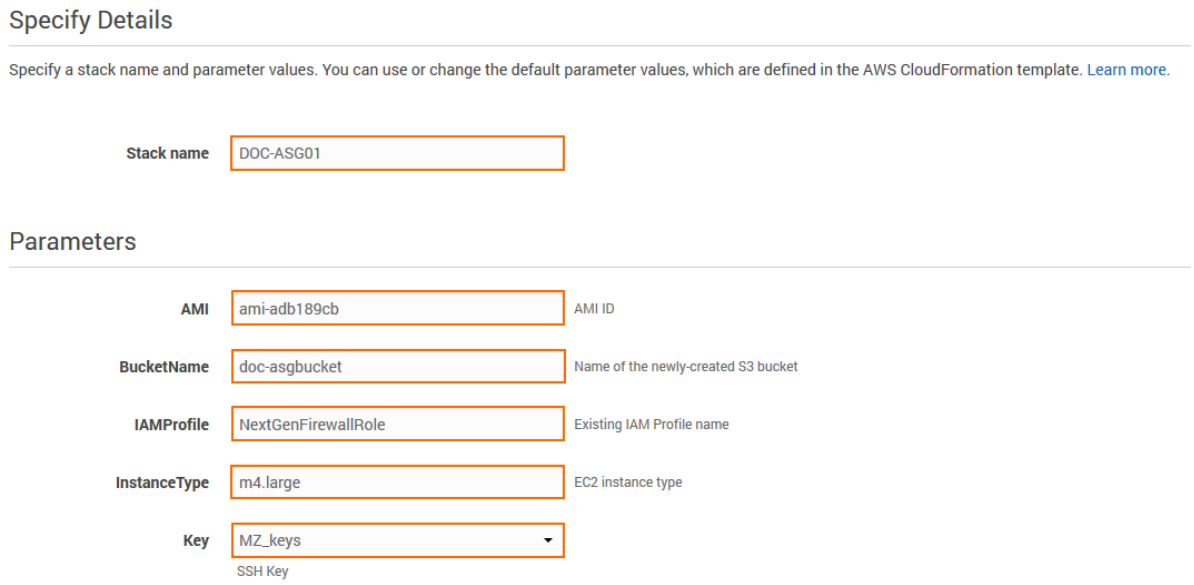
CloudFormation templates can be deployed via the AWS web console, CLI, REST, or PowerShell.

1. Log into the AWS console.
2. Click **Services** and select **CloudFormation**.
3. Click **Create Stack**

4. Select **Upload a template to Amazon S3**.
5. Click **Browse** and select the template file.

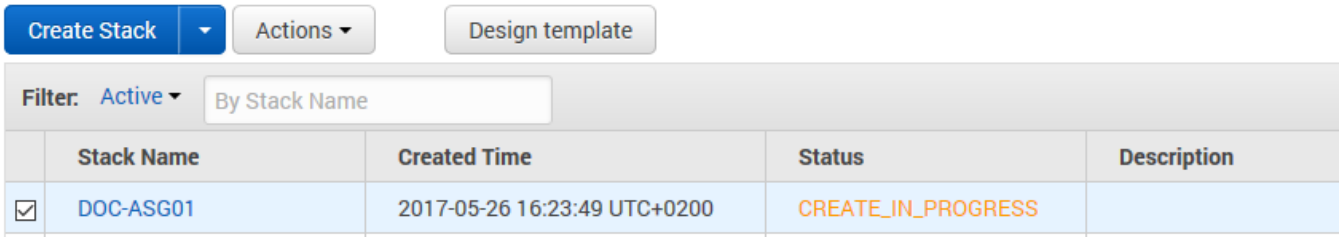


6. Click **Next**.
7. Enter the **Stack name**.
8. Fill in the template **Parameters**.
   - **Stack Name** – Enter a name.
   - **AMI** – Enter the ID for the Barracuda CloudGen Firewall PAYG AMI for your AWS region.
   - **BucketName** – Enter the name for the S3 bucket used to store the firewall configuration.
   - **IAMProfile** – Enter the IAM role created for the CloudGen Firewall.
   - **InstanceType** – Enter a supported instance type. Default `m4.large`.
   - **Key** – Select the key pair from the list. You must have access to the private key of the selected key pair to log in via SSH.



9. Click **Next**.
10. (optional) Enter **Tags** for your stack.
11. In the **Advanced** section, set additional options for your stack:
    - **Notification options**
    - **Timeout** – Set the timeout in minutes.
    - **Rollback on failure** – When set to **yes**, the deployment will be rolled back if any errors are encountered.
12. Click **Next**.
13. Review the settings and click **Create**.

The resources defined in the template are now deployed. This may take a couple of minutes. When the **Status** column shows **CREATE_COMPLETE**, the template has been deployed successfully. If the firewall fetches a PAR file from a Control Center, it may take a couple of minutes for the firewall to be available.



Step 4. Configure Log Streaming to AWS CloudWatch

Log files are generated and stored on each firewall instance in the Auto Scaling Group. To aggregate and store the log files generated on the firewall cluster, configure the CloudGen Firewall cluster to

stream all logs to AWS CloudWatch.

For more information, see How to Configure Log Streaming to AWS CloudWatch.

Figures

1. aws_autoscale_cluster_plain.png
2. awsIG_list_AMIs.png
3. aws_deploy_00.png
4. aws_cloudformation_01.png
5. aws_cloudformation_02.png
6. aws_cloudformation_03.png
7. aws_cloudformation_04.png
8. aws_cloudformation_05.png
9. aws_cloudformation_06.png
10. aws_cloudformation_07.png
11. aws_cloudformation_08.png
12. aws_cloudwatch_logs.png