

## How to Configure Scaling Policies for a CloudGen Firewall Auto Scaling Cluster

<https://campus.barracuda.com/doc/73719779/>

Scaling policies are required for the firewall cluster to adjust the capacity in response to changes in demand. Define CloudWatch alarms for the high and low thresholds. Use the custom metrics collected from the firewall cluster or the default EC2 system metrics. Add scaling policies to the Auto Scaling group that trigger a scaling action when the health check is in alarm state.

### Custom Metrics

The firewall published the following custom metrics in 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

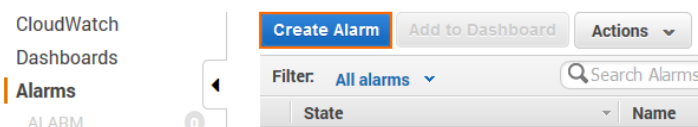
#### Custom Firewall Metrics

- 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

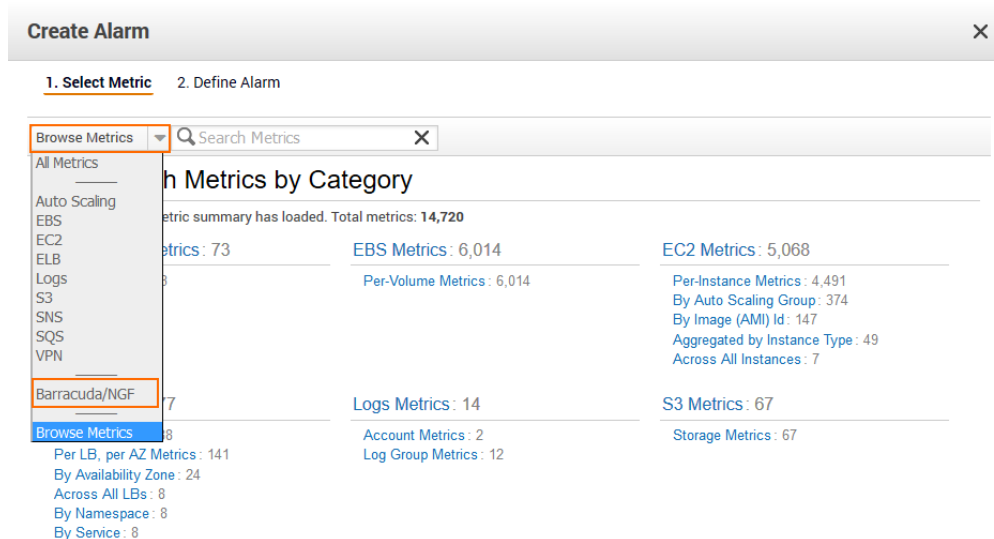
## Step 1. Create CloudWatch Alarm

Create two CloudWatch alarms, one for the high and one for the low alarm threshold.

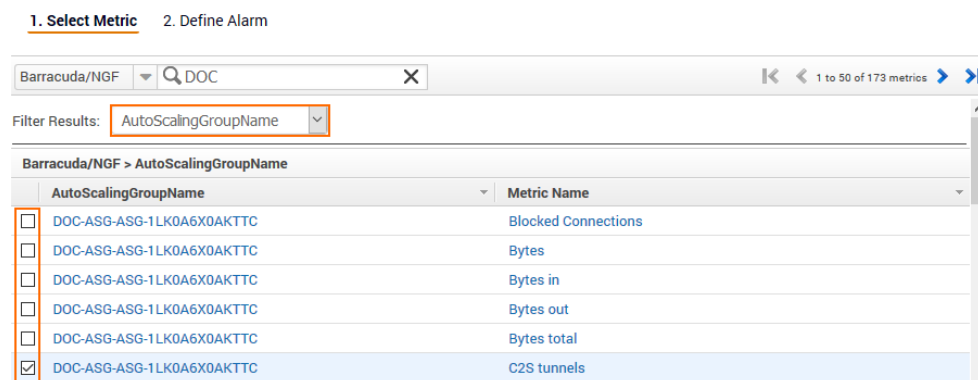
1. Log into the AWS console.
2. Click **Services** and select **CloudWatch**.
3. In the left menu, click **Alarms**.
4. Click **Create Alarm**.



5. From the **Browse Metrics** drop-down list, select **Barracuda/NGF**.



6. From the **Filter Results** drop-down list, select **AutoScalingGroupName**.
7. Select the check box for the metric.



8. Click **Next**.
9. Enter a **Name**.
10. Configure the **Alarm Threshold**:
  - **Logic operator** - Select **>=** when defining an alarm to scale out, **<=** when defining and alarm to scale in.

- **Alarm threshold** – Depending on the instance and metric type, enter the threshold. If unsure, use CloudWatch to monitor your cluster under load to determine the correct value to match your workload.
- **Period** – Enter the time period the threshold must be exceeded for alarm to be triggered.

## Alarm Threshold

Provide the details and threshold for your alarm. Use the graph on the right to help set the appropriate threshold.

**Name:**

**Description:**

---

**Whenever:** C2S tunnels

**is:**

**for:**  consecutive period(s)

11. In the **Alarms section**, click **delete** to not receive a notification when the alarm is triggered. Alternatively, select an SNS topic that is configured to send notification emails when the alarm is triggered.

### Actions

Define what actions are taken when your alarm changes state.

Notification

Delete

**Whenever this alarm:**

**Send notification to:**  [New list](#) [Enter list](#) ⓘ

This notification list is managed in the SNS console.

+ Notification

+ AutoScaling Action

+ EC2 Action

12. From the **Period** drop-down list, select the number of minutes.
13. From the Statistics drop-down list, select **Average** or **Sum** depending on the metric.
14. Click **Create Alarm**.

The alarm is in the **INSUFFICIENT** state until there is enough data for the alarm. As soon as enough data is available, the alarm state changes to **OK** or **Alarm**.

CloudWatch  
 Dashboards  
**Alarms**  
 ALARM  
 INSUFFICIENT 13  
 OK  
 Billing

Create Alarm
 Add to Dashboard
 Actions

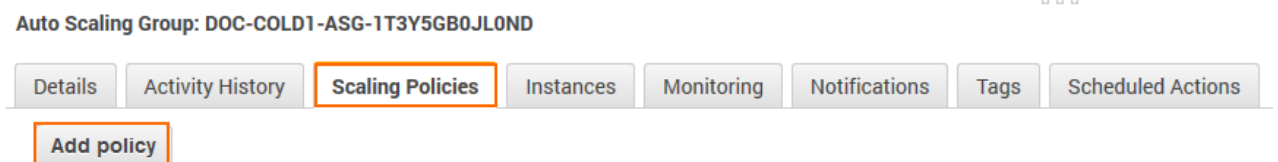
Filter: All alarms
 Search Alarms

State	Name	Threshold	Config Status
<input checked="" type="checkbox"/> INSUFFICIENT_DATA	DOC-NGFScaleOutAlarm	C2S tunnels >= 350 for 2 minutes	No actions

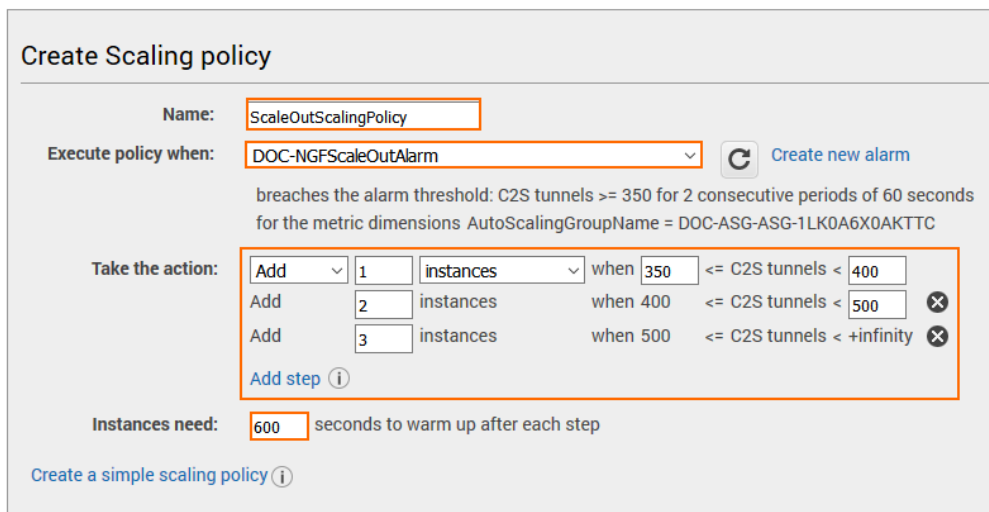
## Step 2. Add Scaling Policy to Scale Out

1. Log into the AWS console.

2. Click **Services** and select **EC2**.
3. In the left menu, click **Auto Scaling Groups**.
4. Select the CloudGen Firewall Auto Scaling group.
5. In the lower half, click the **Scaling Policies** tab.
6. Click **Add policy**.



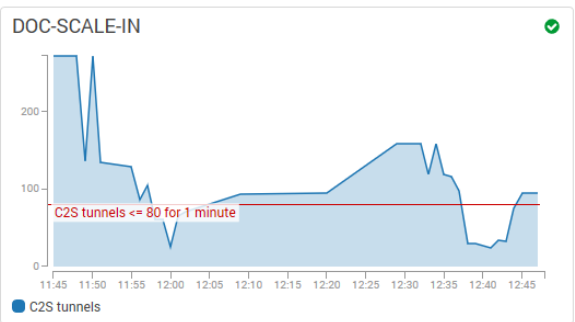
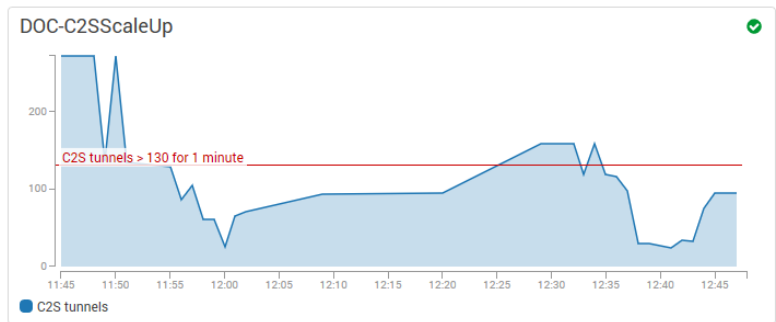
7. Enter a **Name**.
8. From the **Execute policy when** drop-down list, select the matching CloudWatch alarm created in Step 1.
9. Configure the action:
  - **Action** – Select **add** to scale out, or **Remove** to scale in. Click **set** to use an explicit number of instances.
  - **Number of instances** – Depending on the action, enter the number of instances to scale (add / remove) or the number of instances to scale to (set).
10. (optional) Click **add steps** to define a more granular scaling policy that takes into account by how much the threshold is exceeded.
11. In the **Instances need** text box, enter the number of seconds to wait before the next scaling action.



The screenshot shows the 'Create Scaling policy' form. The 'Name' field is 'ScaleOutScalingPolicy'. The 'Execute policy when' dropdown is 'DOC-NGFScaleOutAlarm'. Below this, it says 'breaches the alarm threshold: C2S tunnels >= 350 for 2 consecutive periods of 60 seconds for the metric dimensions AutoScalingGroupName = DOC-ASG-ASG-1LK0A6X0AKTTC'. The 'Take the action' section has three rows, each with 'Add' in the dropdown, a number in a text box, 'instances' in the dropdown, and a condition. The first row is '1 instances when 350 <= C2S tunnels < 400'. The second row is '2 instances when 400 <= C2S tunnels < 500'. The third row is '3 instances when 500 <= C2S tunnels < +infinity'. There is an 'Add step' button and an information icon. The 'Instances need' field is '600' seconds to warm up after each step. At the bottom, there is a link 'Create a simple scaling policy' with an information icon.

12. Click **Create**.

Repeat this for both Scale In and Scale Out policies. Use CloudWatch dashboard widgets to visualize the alarm thresholds



## Figures

1. aws\_scaling\_policies\_01.png
2. aws\_scaling\_policies\_02.png
3. aws\_scaling\_policies\_03.png
4. aws\_scaling\_policies\_04.png
5. aws\_scaling\_policies\_05.png
6. aws\_scaling\_policies\_07.png
7. aws\_scaling\_policies\_08.png
8. aws\_scaling\_policies\_09.png
9. awsIG\_cloudwatch\_monitor\_alarms.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.