How to Manually Configure Cloud Integration for AWS

https://campus.barracuda.com/doc/73719776/

To allow an on-premises firewall or a firewall not running in AWS to connect to AWS services such as AWS CloudWatch, you must manually configure authentication credentials. For firewalls running in AWS, use IAM roles instead. Cloud integration allows your firewall to exchange information with the underlying cloud platform for things like streaming logs to AWS CloudWatch. The IAM user uses the same IAM policies that are assigned to the AWS IAM role.

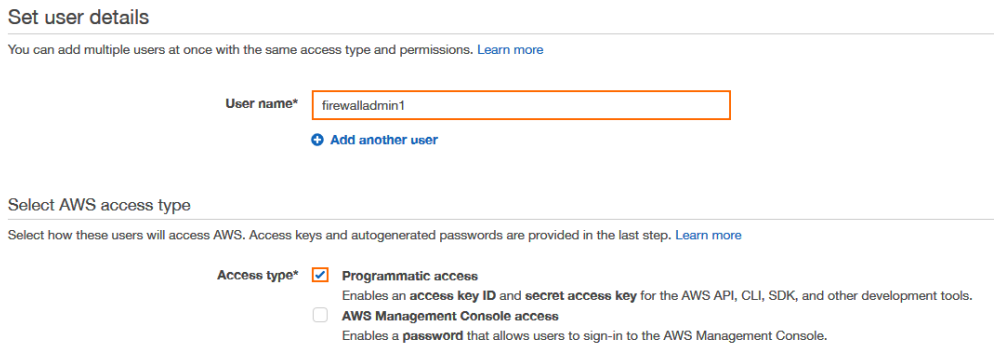
Before You Begin

Create the required IAM policies for your firewall. For more information, see How to Create an IAM Role for a CloudGen Firewall in AWS.

Step 1. Create the IAM User

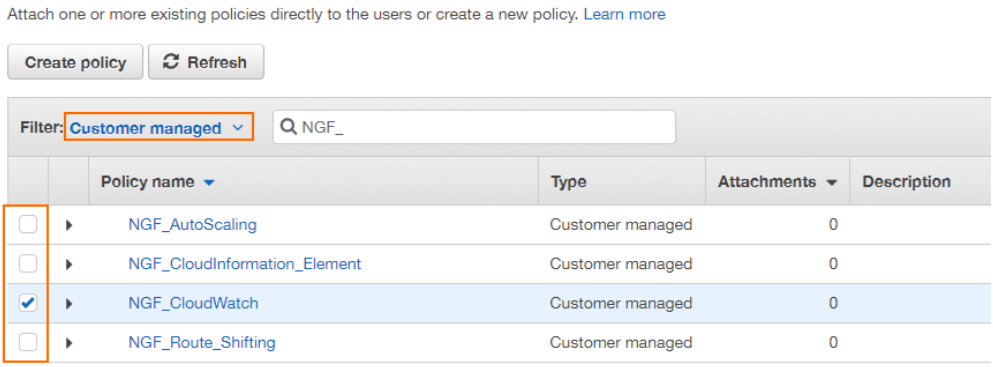
Create the IAM user that is used to connect the firewall instance to the cloud fabric.

1. Go to AWS IAM: https://console.aws.amazon.com/iam.
2. In the left menu, click **Users**.
3. Click **Create New Users**.
4. Enter the **User name**.
5. In the **Select AWS access type** section, select the **Programmatic access** check box.



6. Click **Next: Permissions**.
7. Click **Attach existing policies directly**.

8. From the **Filter** drop-down list, select **Customer Managed**.
9. Select the IAM policies required for the AWS services you need to access. E.g., **NGF_CloudWatch** to send logs to AWS CloudWatch



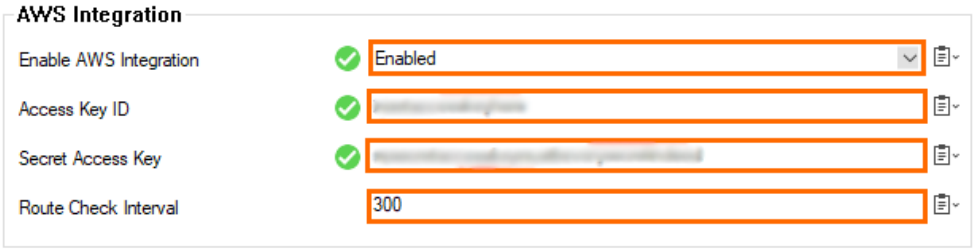
10. Click **Next: Review**.
11. Review the settings, and click **Create user**.
12. Download or click **show** to write down the user's security credentials (access key ID and secret access key)**.**

Step 2. Configure Cloud Integration

Add the access key ID and secret access key to allow the firewall to connect to the AWS cloud fabric.

1. Log into the firewall instance.
2. Go to **CONFIGURATION > Configuration Tree > Box > Advanced Configuration > Cloud Integration**.

3. Click **Lock**.
4. In the left menu, click **AWS Integration**.
5. From the **Enable AWS Integration** list, select **Enabled**.
6. Enter the **Access Key ID** from the IAM user created in Step 1.
7. Enter the **Secret Access Key** from the IAM user created in Step 1.
8. Enter a **Route Check Interval** between 10 and 300 seconds.



9. Click **Send Changes** and **Activate**.

The firewall instance can now connect to the AWS APIs allowed by the IAM policies.

Next Steps

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

Figures

1. AWS_IAM_01.png
2. AWS_IAM_02.png
3. AWS_IAM_03.png
4. AWS_IAM_04.png
5. aws_integration_2020.png