How to Create an IAM Role for an F-Series Firewall in AWS

https://campus.barracuda.com/doc/67175123/

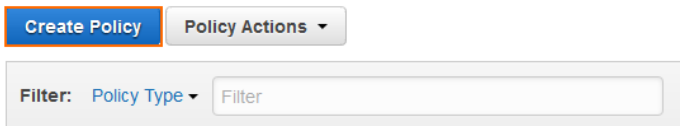
IAM roles are the preferred method for NextGen Firewall instances in AWS to authenticate against AWS APIs. For each feature that requires direct access to AWS resources, a customized IAM policy must be created. These policies are then attached to the IAM role assigned to the instance during deployment. It is possible, to change the IAM policies attached to the IAM role on the fly. If an Access Key ID and Secret Access Key are configured in AWS cloud integration, they take precedence over the IAM role attached to the instance. In order to use all firewall features, the following IAM security policies must be created and attached to the IAM role:

- Cloud Information element
- Route shifting (includes Cloud Information dashboard element)
- AWS CloudWatch streaming
- AWS Auto Scaling or cold standby S3 bucket access

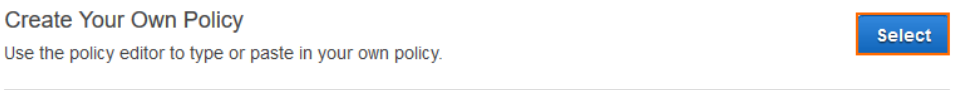
Step 1. Create IAM Policy for Route Shifting

Create an IAM policy to allow route shifting.

1. Log into the AWS console.
2. Click **Services** and select **IAM**.
3. In the left menu, click **Policies**.
4. Click **Create Policy**.



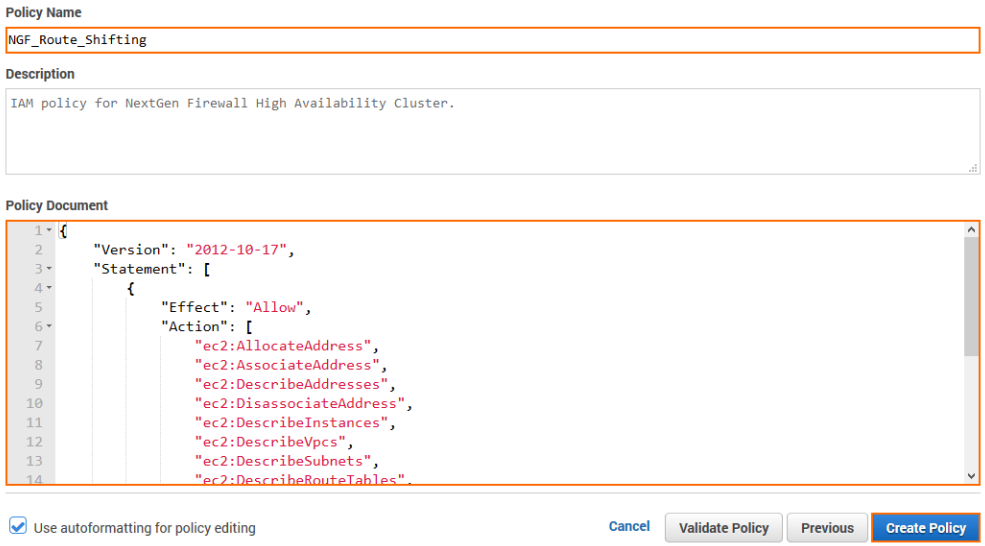
5. Next to **Create Your Own Policy**, click **Select**.



Configure the IAM policy:

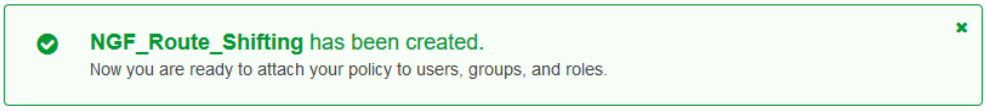
- **Policy Name** – Enter a name for the policy.
- **(optional) Description**
- **Policy Document** – Copy and paste the following policy:

```
{ "Version": "2012-10-17", "Statement": [ { "Effect": "Allow", "Action":
[ "ec2:AllocateAddress", "ec2:AssociateAddress",
"ec2:DescribeAddresses", "ec2:DisassociateAddress",
"ec2:DescribeInstances", "ec2:DescribeVpcs", "ec2:DescribeSubnets",
"ec2:DescribeRouteTables", "ec2:DeleteRoute", "ec2:CreateRoute",
"ec2:DescribeNetworkInterfaces" ], "Resource": [ "*" ] } ] }
```



6. Click **Create Policy**.

The IAM policy for route shifting is now available to be assigned to an IAM role for the NextGen Firewall.

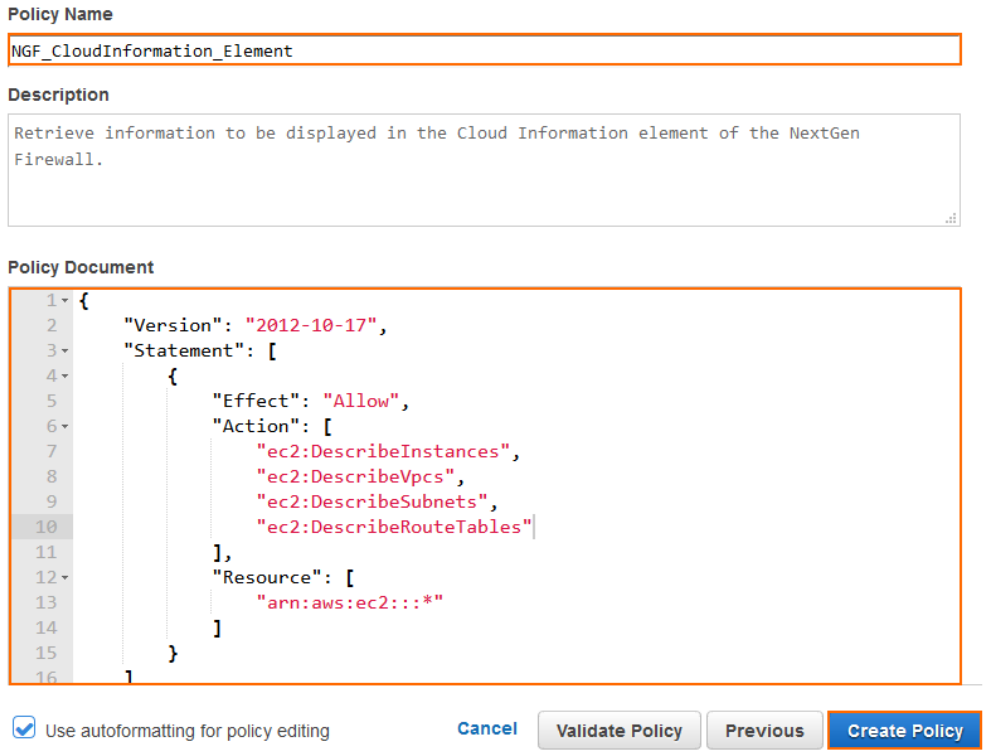


Step 2. Create IAM Policy for the Cloud Information Dashboard Element

Create this policy only if you are not using the route shifting IAM policy. The route shifting IAM policy includes all permissions necessary for the Cloud Information element.

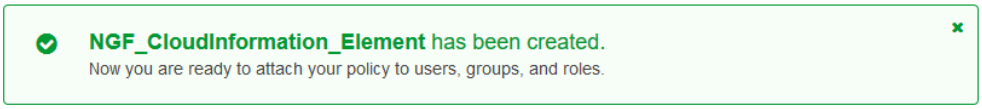
1. Log into the AWS console.
2. Click **Services** and select **IAM**.
3. In the left menu, click **Policies**.
4. Click **Create Policy**.
5. Next to **Create Your Own Policy**, click **Select**.
   Configure the IAM policy:
   - **Policy Name** – Enter a name for the policy.
   - **(optional) Description**
   - **Policy Document** – Copy and paste the following policy:

```
{ "Version": "2012-10-17", "Statement": [ { "Effect": "Allow", "Action": [ "ec2:DescribeInstances", "ec2:DescribeVpcs", "ec2:DescribeSubnets", "ec2:DescribeRouteTables" ], "Resource": [ "arn:aws:ec2:::*" ] } ] }
```



6. Click **Create Policy**.

The IAM policy for the Cloud Information element is now available to be assigned to an IAM role for the NextGen Firewall.



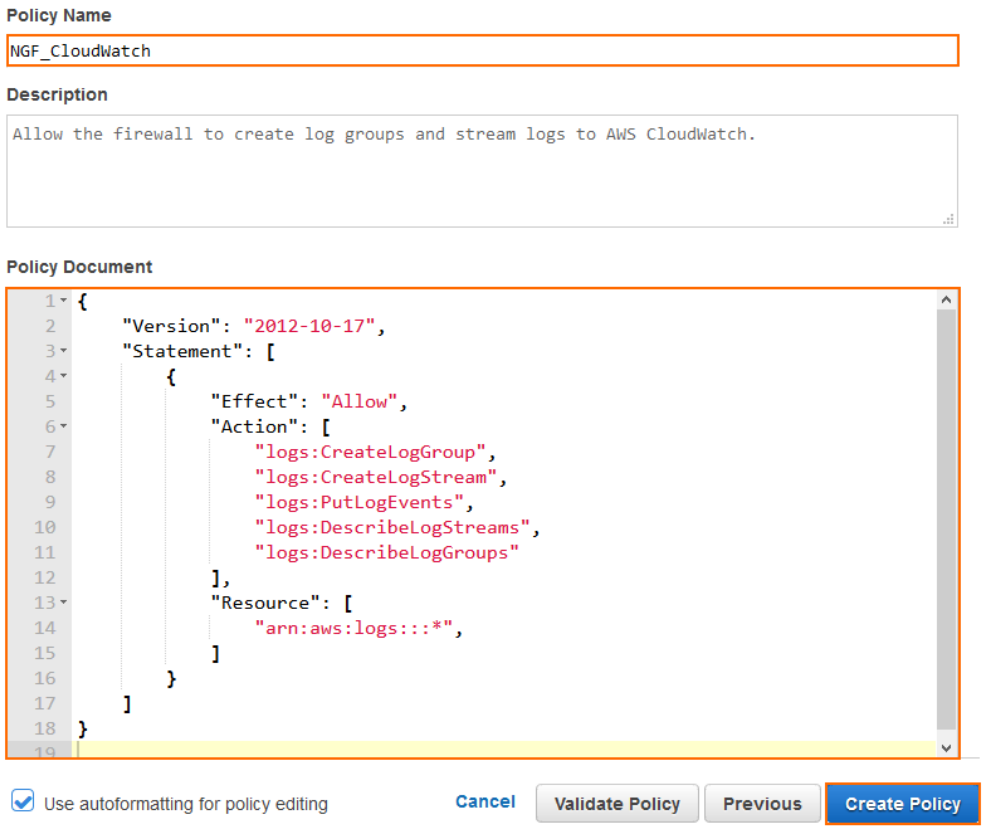
Step 3. Create IAM Policy for Log Streaming to AWS CloudWatch

This IAM policy grants the firewall the necessary permissions to stream logs to AWS CloudWatch.

1. Log into the AWS console.
2. Click **Services** and select **IAM**.
3. In the left menu, click **Policies**.
4. Click **Create Policy**.
5. Next to **Create Your Own Policy**, click **Select**.
6. Configure the IAM policy:
   - **Policy Name** – Enter a name for the policy.
   - **(optional) Description**
   - **Policy Document** – Copy and paste the following policy:

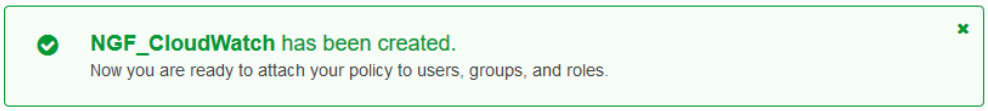
```
{ "Version": "2012-10-17", "Statement": [ { "Effect": "Allow", "Action":
```

```
[ "logs:CreateLogGroup", "logs:CreateLogStream", "logs:PutLogEvents",
"logs:DescribeLogStreams", "logs:DescribeLogGroups" ], "Resource": [
"arn:aws:logs:*:*:*" ] } ] }
```



7. Click **Create Policy**.

The IAM policy for streaming logs to AWS CloudWatch is now available to be assigned to an IAM role for the NextGen Firewall.



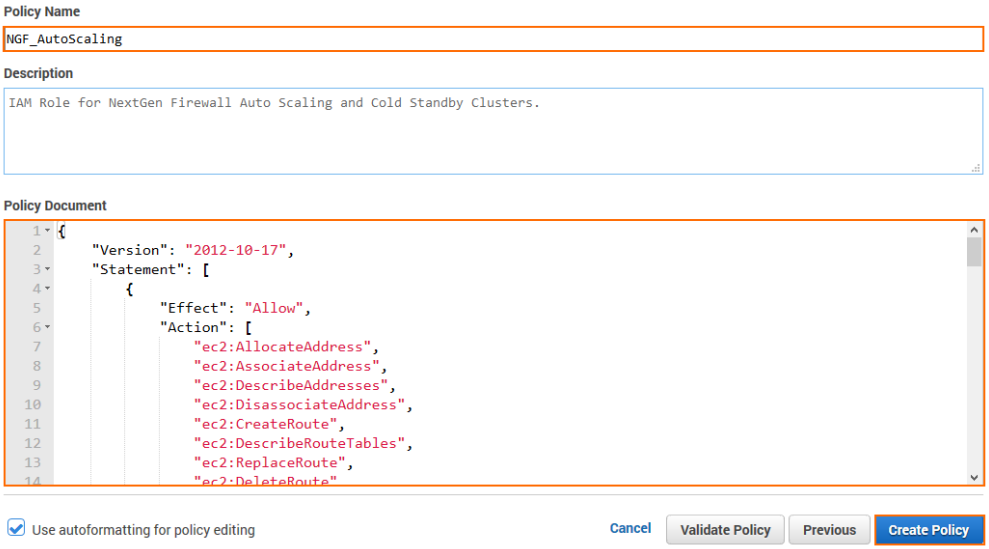
Step 4. Create IAM Policy for AWS Auto Scaling Group Deployments

This IAM policy grants the necessary permissions for Auto Scaling and cold standby architectures for the NextGen Firewall.

1. Log into the AWS console.
2. Click **Services** and select **IAM**.
3. In the left menu, click **Policies**.
4. Click **Create Policy**.

5. Next to **Create Your Own Policy**, click **Select**.
6. Configure the IAM policy:
   - **Policy Name** – Enter a name for the policy.
   - **(optional) Description**
   - **Policy Document** – Copy and paste the following policy:


```
{ "Version": "2012-10-17", "Statement": [ { "Effect": "Allow", "Action":
[ "ec2:AllocateAddress", "ec2:AssociateAddress",
"ec2:DescribeAddresses", "ec2:DisassociateAddress", "ec2:CreateRoute",
"ec2:DescribeRouteTables", "ec2:ReplaceRoute", "ec2:DeleteRoute",
"ec2:CreateTags", "ec2:DescribeInstances", "ec2:DeleteTags",
"ec2:DescribeTags", "ec2:ModifyInstanceAttribute" ], "Resource": "*" },
{ "Effect": "Allow", "Action": [ "autoscaling:CreateOrUpdateTags",
"autoscaling:DeleteTags", "autoscaling:DescribeAutoScalingGroups",
"autoscaling:DescribeAutoScalingInstances", "autoscaling:DescribeTags",
"autoscaling:SetInstanceProtection" ], "Resource": "*" }, { "Action": [
"sqs:CreateQueue", "sqs:DeleteMessage", "sqs:DeleteQueue",
"sqs:GetQueueAttributes", "sqs:ReceiveMessage",
"sqs:SetQueueAttributes", "sqs:GetQueueUrl" ], "Effect": "Allow",
"Resource": "arn:aws:sqs:*" }, { "Action": [ "sns:CreateTopic",
"sns:Publish", "sns:Subscribe", "sns:Unsubscribe",
"sns:ListSubscriptionsByTopic" ], "Effect": "Allow", "Resource":
"arn:aws:sns:*" }, { "Action": [ "cloudwatch:PutMetricData" ], "Effect":
"Allow", "Resource": "*" }, { "Action": [ "sts:GetCallerIdentity" ],
"Effect": "Allow", "Resource": "*" }, { "Effect": "Allow", "Action": [
"s3:CreateBucket", "s3:ListBucket", "s3:PutBucketVersioning",
"s3:PutObject", "s3:GetBucketVersioning", "s3:ListBucketVersions",
"s3:GetObject", "s3:GetObjectVersion", "s3:DeleteObjectVersion" ],
"Resource": "arn:aws:s3:::*" } ] }
```

7. Click **Create Policy**.

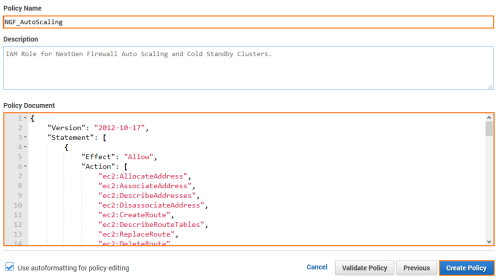
The IAM policy for AWS Auto Scaling and cold standby architectures is now available to be assigned to

an IAM role for the NextGen Firewall.

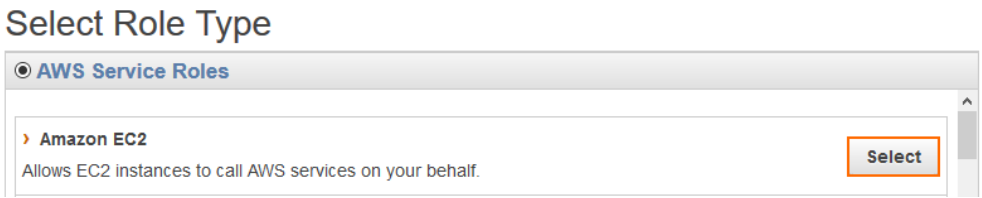
Step 5. Create the IAM Role

Create the IAM role and assign the IAM policies for all NextGen Firewall Cloud Integration features used by the firewall Instance.

1. Log into the AWS console.
2. Click **Services** and select **IAM**.
3. In the left menu, click **Roles**.
4. Click **Create New Role**.

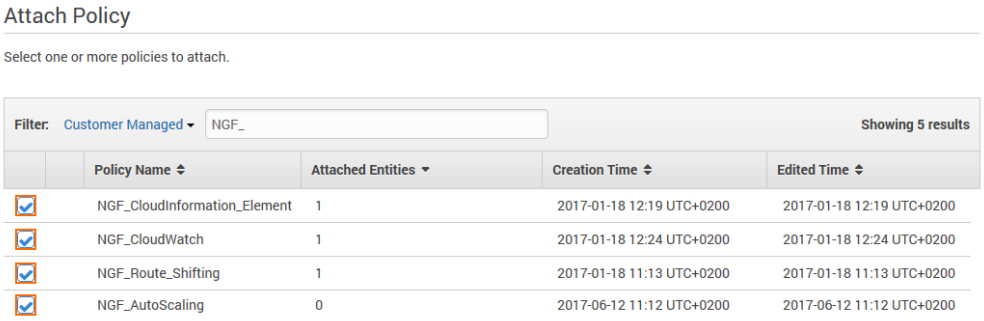


5. Enter the **Role Name**.
6. Click **Next Step**.
7. In the **AWS Service Roles** section, next to **Amazon EC2** click **Select**.



8. Select the IAM firewall policies you just created.

   Select the policies only for features that will be used in the deployed firewall instance. You can change the attached IAM policies later if required.



9. Click **Next Step**.
10. Review the settings and click **Create Role**.

Assign this role to the NextGen Firewall instance during deployment.

Figures

1. aws_IAM_role_01.png
2. aws_IAM_role_02.png
3. aws_IAM_role_03.png
4. aws_IAM_role_04.png
5. aws_IAM_role_05.png
6. aws_IAM_role_06.png
7. aws_IAM_role_07.png
8. aws_IAM_role_08.png
9. aws_IAM_role_09.png
10. iam_policy_autoscaling_done.png
11. aws_IAM_role_09.png
12. aws_IAM_role_10.png
13. aws_IAM_role_11.png