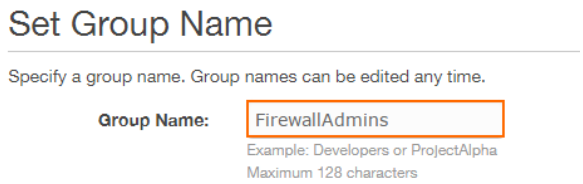
How to Configure Cloud Integration for AWS

https://campus.barracuda.com/doc/49058718/The AWS route table associated with your backend subnets allows you to configure the Instance that is used as the default gateway for the route. For the firewall to be able to forward traffic, the source/destination check of the network interface (ENI) must be disabled. Using IAM credentials, the firewall Instance can connect to the cloud fabric and change the routing table on the fly when the virtual server fails over from one firewall Instance to the other.

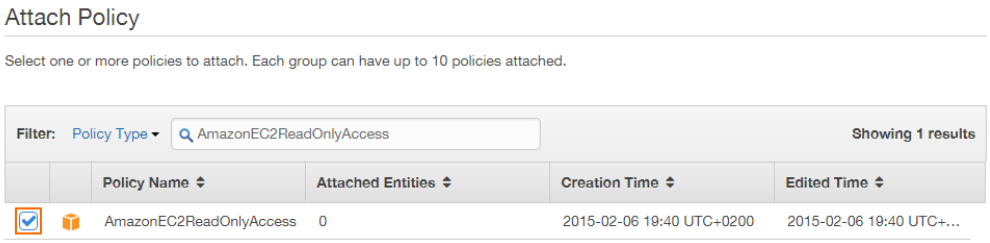
Step 1. Configure IAM credentials

Create an IAM user with the necessary permissions for the firewall to connect to the cloud fabric.

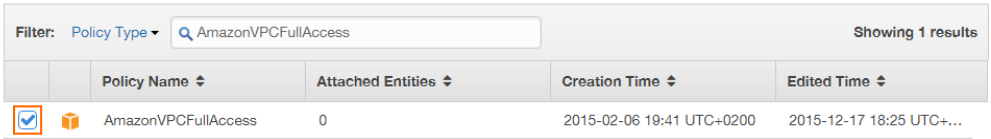
1. Go to AWS IAM (https://console.aws.amazon.com/iam).
2. In the left menu, click **Groups**.
3. Click **Create New Groups**.
4. Enter a **Group Name**.



5. Click **Next Step**.
6. Attach the following policies to the group:
   - **AmazonEC2ReadOnlyAccess** – Required for cloud integration dashboard element.



   - **AmazonVPCFullAccess** – Required to read and rewrite AWS route tables.

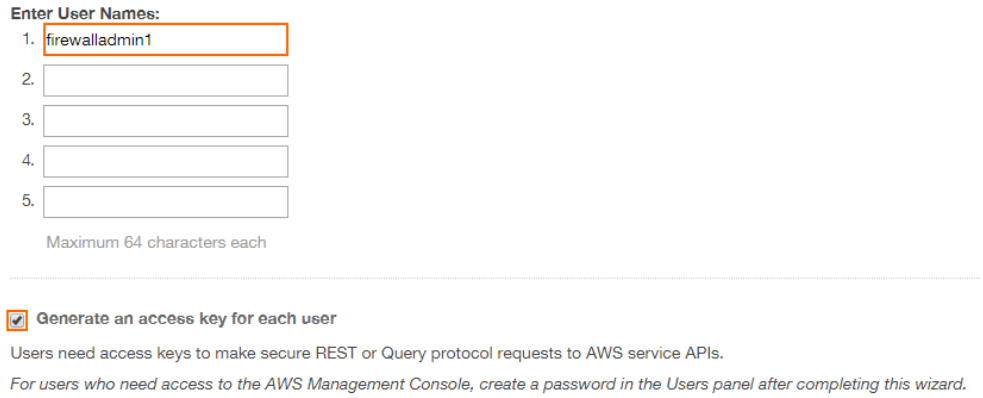


7. Click **Next Step**.
8. Click **Create Group**.

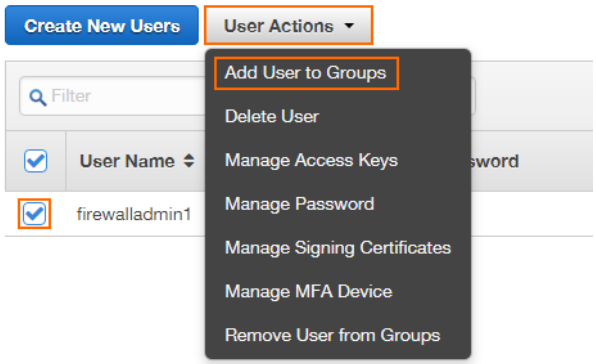
Step 2. Create IAM user

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

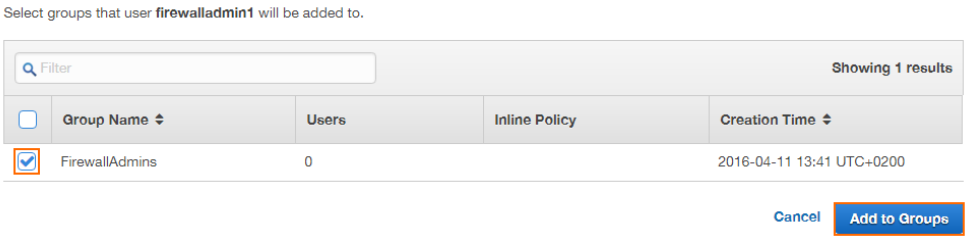
1. Go to AWS IAM (https://console.aws.amazon.com/iam).
2. In the left menu, click **Users**.
3. Click **Create New Users**.
4. Enter the username in the list.
5. Select the check box to **Generate an access key for each user**.



6. Click **Create**.
7. Download or write down the user's security credentials (Access Key ID and Secret Access Key)**.**
8. Select the IAM user you just created and select **Add User to Group** from the **User Actions** list.



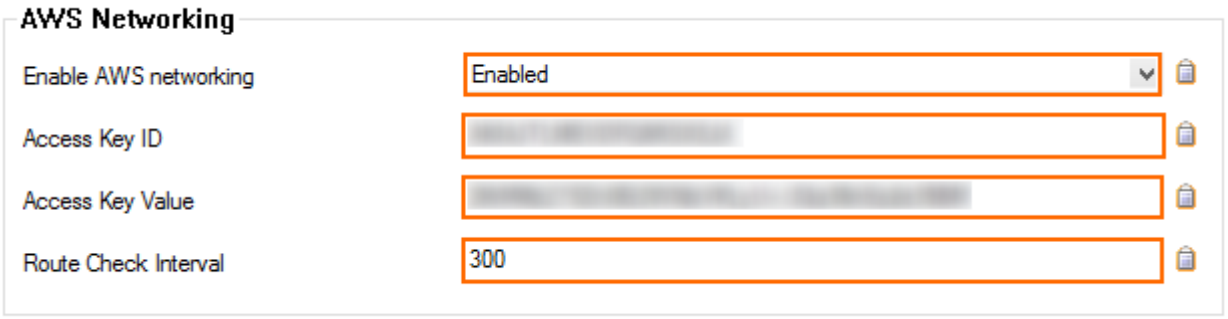
9. Select the IAM group you created in step 1 and click **Add to Groups**.



Step 3. Configure cloud integration

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

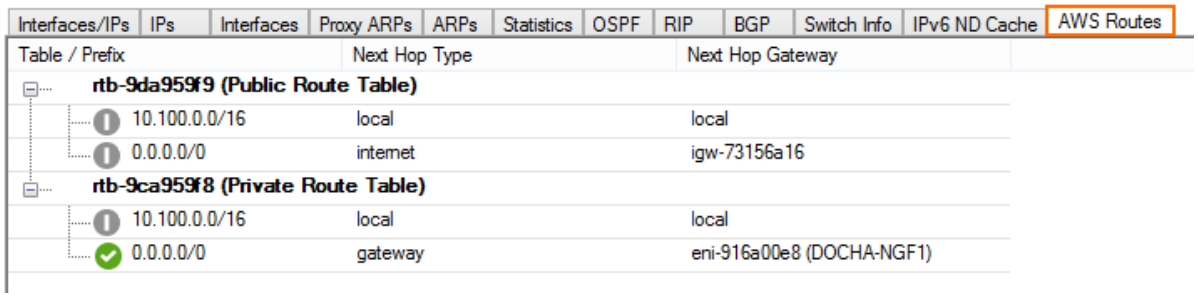
1. Log in to the firewall Instance.
2. Go to **CONFIGURATION > Configuration Tree > Box > Advanced Configuration > Cloud Integration**.
3. Click **Lock**.
4. In the left menu, click **AWS Networking**.
5. From the **Enable AWS networking** list, select **Enabled**.
6. Enter the **Access Key ID** from the IAM user created in step 2.
7. Enter the **Access Key Value** from the IAM user created in step 2.
8. Enter the **Route Check Interval** between 10 and 300 seconds.



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

The firewall Instance can now connect to the AWS cloud fabric to query the information necessary for the cloud element on the **DASHBOARD** and the AWS route table.

To see the AWS route table, go to **CONTROL > Networking > AWS Routes**.


Interfaces/IPs
IPs
Interfaces
Proxy ARPs
ARPs
Statistics
OSPF
RIP
BGP
Switch Info
IPv6 ND Cache
AWS Routes
Table / Prefix
Next Hop Type
Next Hop Gateway
rtb-9da959f9 (Public Route Table)
10.100.0.0/16
local
local
0.0.0.0/0
internet
igw-73156a16
rtb-9ca959f8 (Private Route Table)
10.100.0.0/16
local
local
0.0.0.0/0
gateway
eni-916a00e8 (DOCHA-NGF1)

Figures

1. AWS_IAM_01.png
2. AWS_IAM_02.png
3. AWS_IAM_03.png
4. AWS_IAM_04.png
5. AWS_IAM_05.png
6. AWS_IAM_06.png
7. aws_cloud_integration_01.png
8. aws_cloud_integration_03.png
9. aws_cloud_integration_02.png