

## 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**.

#### Set Group Name

Specify a group name. Group names can be edited any time.

Group Name:

Example: Developers or ProjectAlpha  
Maximum 128 characters

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

Attach Policy

Select one or more policies to attach. Each group can have up to 10 policies attached.

Filter:	Policy Type	AmazonEC2ReadOnlyAccess	Showing 1 results	
	Policy Name	Attached Entities	Creation Time	Edited Time
<input checked="" type="checkbox"/>	AmazonEC2ReadOnlyAccess	0	2015-02-06 19:40 UTC+0200	2015-02-06 19:40 UTC+...

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

Filter:	Policy Type	AmazonVPCFullAccess	Showing 1 results	
	Policy Name	Attached Entities	Creation Time	Edited Time
<input checked="" type="checkbox"/>	AmazonVPCFullAccess	0	2015-02-06 19:41 UTC+0200	2015-12-17 18:25 UTC+...

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**.

Enter User Names:

1.
2.
3.
4.
5.

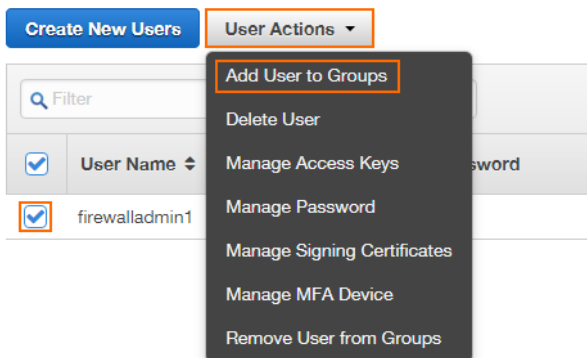
Maximum 64 characters each

**Generate an access key for each user**

Users need access keys to make secure REST or Query protocol requests to AWS service APIs.

*For users who need access to the AWS Management Console, create a password in the Users panel after completing this wizard.*


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.



The screenshot shows the 'Create New Users' wizard in the AWS IAM console. The 'User Actions' dropdown menu is open, and the 'Add User to Groups' option is selected. The user 'firewalladmin1' is listed in the table below the dropdown.

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

Select groups that user **firewalladmin1** will be added to.



The screenshot shows the 'Add to Groups' dialog box in the AWS IAM console. The 'FirewallAdmins' group is selected in the table. The 'Add to Groups' button is highlighted.







Group Name	Users	Inline Policy	Creation Time
<input checked="" type="checkbox"/> FirewallAdmins	0		2016-04-11 13:41 UTC+0200

### 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.

**AWS Networking**

Enable AWS networking	Enabled	
Access Key ID		
Access Key Value		
Route Check Interval	300	

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.

☰ CLOUD INFORMATION		⚙
Cloud Integration	Configured	→
Hosting Cloud	Amazon EC2	
Instance Id		→
Instance Name	DOCHA-NGF2	
Instance Type	m3.medium	
Public IP Address		
Region/Availability Zone	eu-west-1/eu-west-1c	
VPC/Subnet	DOC-VPC/Public subnet	→

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							
<b>rtb-9da959f9 (Public Route Table)</b>											
	10.100.0.0/16										local
	0.0.0.0/0										igw-73156a16
<b>rtb-9ca959f8 (Private Route Table)</b>											
	10.100.0.0/16										local
	0.0.0.0/0										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

© Barracuda Networks Inc., 2019 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.