



How to Configure AWS Route Tables for Firewalls with Multiple Network Interfaces

For instances in a private subnet to send traffic through the network interface of the firewall in this subnet, you must create an AWS route table for each private subnet. Add a default route using the elastic network interface as the target device. Traffic leaving the VPC is now sent via the network interface of the firewall in the same subnet. However, internal VPC traffic is not sent through the firewall. For more information, see [Segmentation Firewall for Single AZ VPCs](#).

AWS Reference Architectures

This article is used in the following AWS reference architectures:

- [AWS Reference Architecture - Segmentation Firewall for Single AZ VPCs](#)

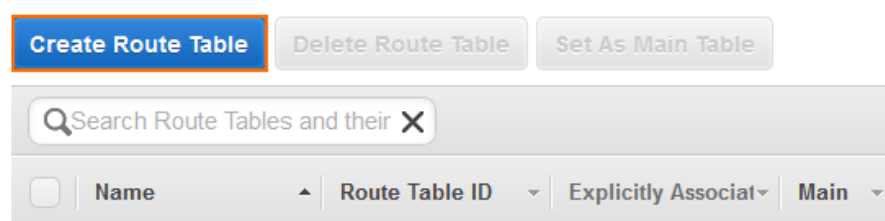
Before You Begin

- Deploy a firewall instance in the public subnet of the VPC.
- The public and private subnets must be in the same Availability Zone.
- Add a network interface in the private subnet to the firewall instance. For more information, see [How to Add AWS Elastic Network Interfaces to a Firewall Instance](#).

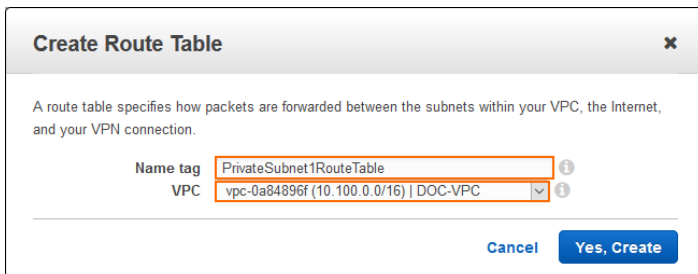
Step 1. Create an AWS Route Table

Create an AWS route table for each private subnet.

1. Log into the AWS console.
2. Click **Services** and select **VPC**.
3. In the **Virtual Private Cloud** section of the left menu, click **Route Tables**.
4. Click **Create Route Table**. The **Create Route Table** popover opens.



5. Configure the route table:
 - o **Name tag** - Enter the name for the route table.
 - o **VPC** - Select the VPC from the list.



6. Click **Yes, Create**.

Step 2. Associate the Private Subnet with the Route Table

If the subnet is not explicitly associated with a route table, the main route table for the VPC is used.



1. Log into the AWS console.
2. Click **Services** and select **VPC**.
3. In the **Virtual Private Cloud** section of the left menu, click **Route Tables**.
4. Select the route table created in step 1.
5. In the lower half of the screen, click on the **Subnet Associations** tab.

<input type="checkbox"/>	Name	Route Table ID	Explicitly Associat	Main	VPC
<input checked="" type="checkbox"/>	PrivateSubnet1RouteTab	rtb-e05f7b84	0 Subnets	No	vpc-0a84896f (10.100.0.0/16) DOC-VPC

rtb-e05f7b84 | PrivateSubnet1RouteTable

Summary Routes **Subnet Associations** Route Propagation Tags

6. Click **Edit**.
7. Select the subnet you want to associate with this route table.
8. Click **Save**.

rtb-e05f7b84 | PrivateSubnet1RouteTable

Summary Routes **Subnet Associations** Route Propagation Tags

Cancel **Save**

Associate	Subnet	CIDR	Current Route Table
<input type="checkbox"/>	subnet-6e06f10a (10.100.0.0/24) DOC Public Subnet #1	10.100.0.0/24	rtb-9da959f9 Public Route Table
<input checked="" type="checkbox"/>	subnet-6d06f109 (10.100.1.0/24) DOC- Private Subnet #1	10.100.1.0/24	rtb-9ca959f8 Private Route Table #1
<input type="checkbox"/>	subnet-834d3fe7 (10.100.2.0/24) DOC Private Subnet #2	10.100.2.0/24	rtb-23613a47 Private Route Table #2

The private subnet is now associated with the route table.

rtb-e05f7b84 | PrivateSubnet1RouteTable

Summary Routes **Subnet Associations** Route Propagation Tags

Edit

Subnet	CIDR
subnet-6d06f109 (10.100.1.0/24) DOC- Private Subnet #1	10.100.1.0/24

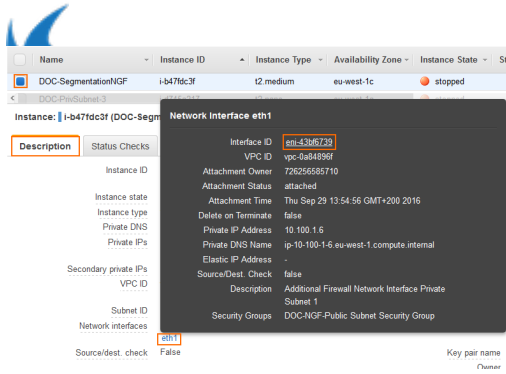
The following subnets have not been explicitly associated with any route tables and are therefore associated with the main route table:

Subnet	CIDR
--------	------

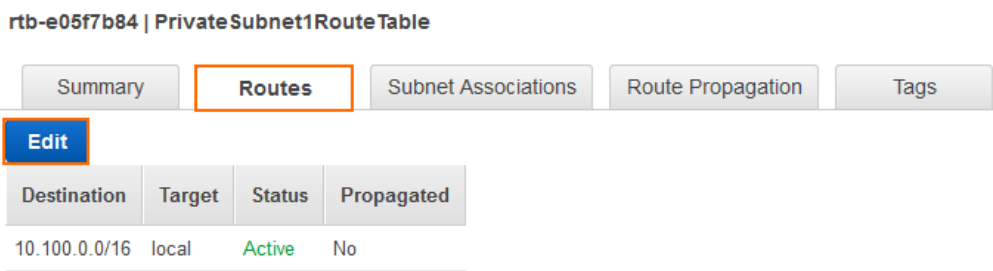
All your subnets are associated with a route table.

Step 2. Add a Default Route with the Network Interface of the Firewall as the Target

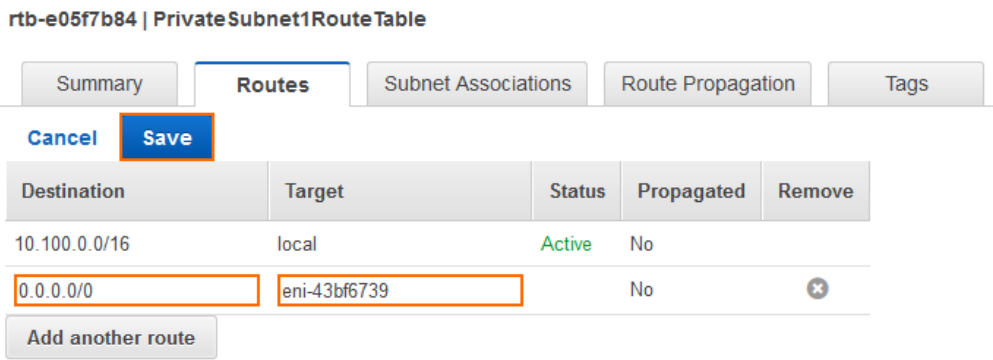
Locate the elastic network interface identifier (eni-12345678) for the network interface in this subnet. Click on the network interface in the **Description** tab of the firewall instance to retrieve the ID.



1. Log into the AWS console.
2. Click **Services** and select **VPC**.
3. In the **Virtual Private Cloud** section of the left menu, click **Route Tables**.
4. Select the route table created in step 1.
5. In the lower half of the screen, click on the **Routes** tab.
6. Click **Edit**.



7. Click **Add another route**.
8. Configure the route:
 - o **Destination** - Enter 0.0.0.0/0.
 - o **Target** - Enter the ID for the firewall network interface located in this subnet.



9. Click **Save**.

All traffic leaving the VPC from the associated subnet is now sent through the firewall. The status of the route must be **Active**.

