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

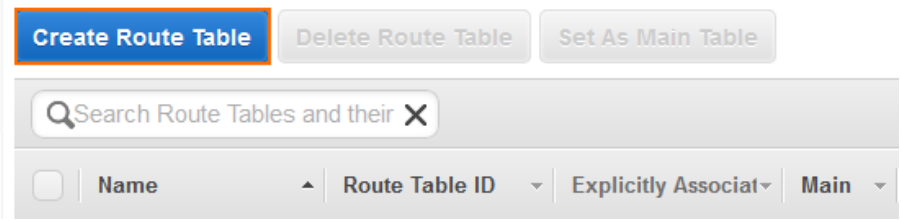
Before You Begin

- 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.

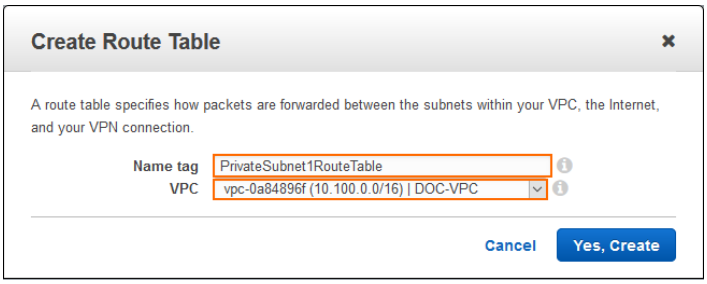
Step 1. Create an AWS Route Table

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

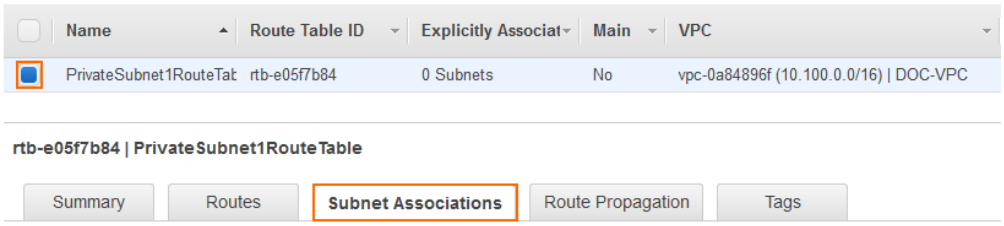


6. Click **Yes, Create**.

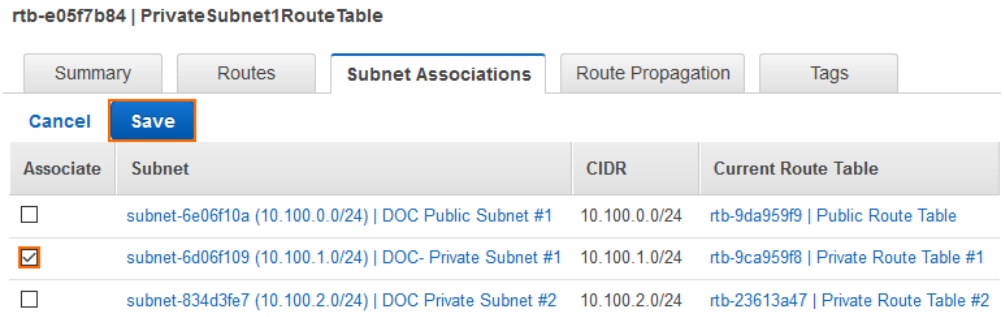
Step 2. Associate the Private Subnet with the Route Table

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

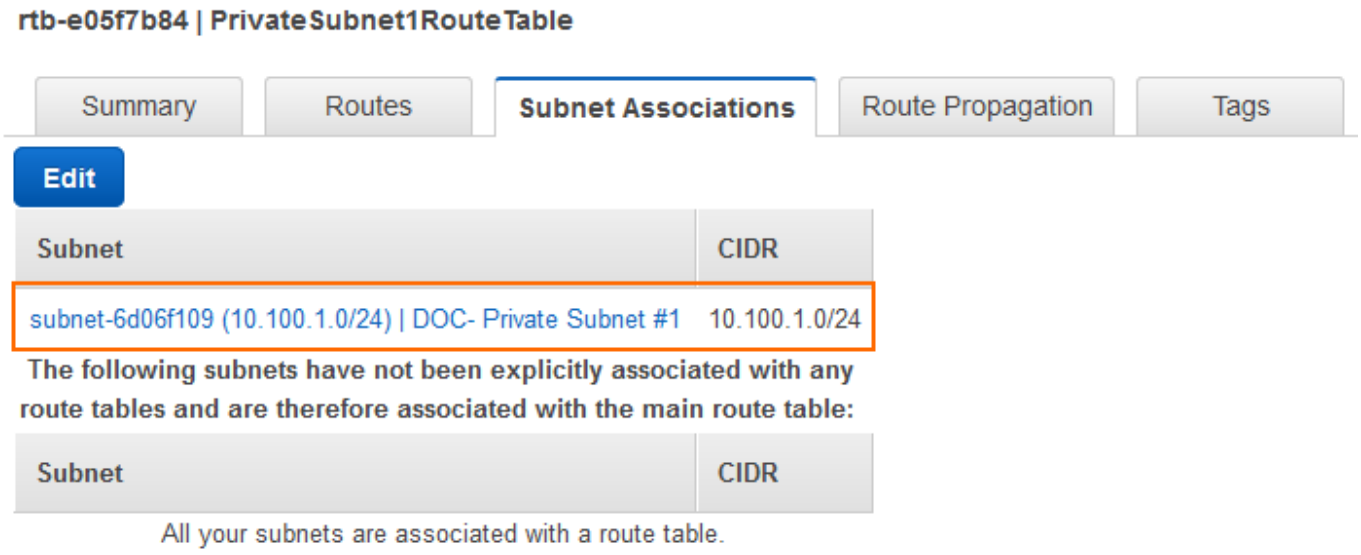
1. Log into the AWS console.
2. Click **Services** and select **VPC**.
3. In the **Virtual Private Cloud** section of the left menu, click **Route Tables**.
4. Select the route table created in step 1.
5. In the lower half of the screen, click on the **Subnet Associations** tab.



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

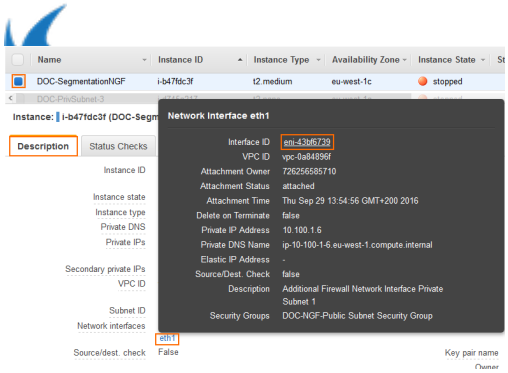


The private subnet is now associated with the route table.

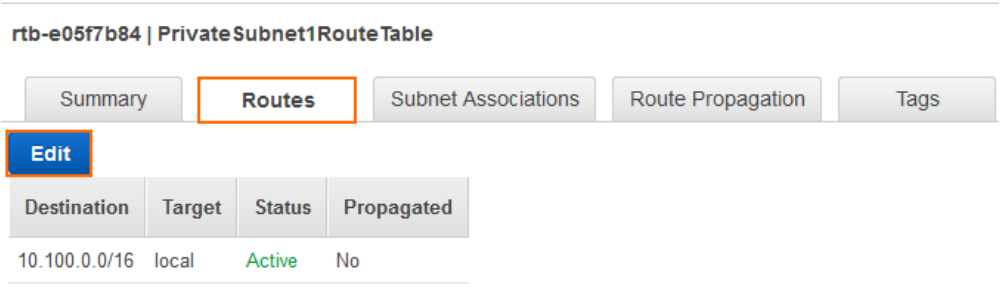


Step 2. Add a Default Route with the Network Interface of the Firewall as the Target

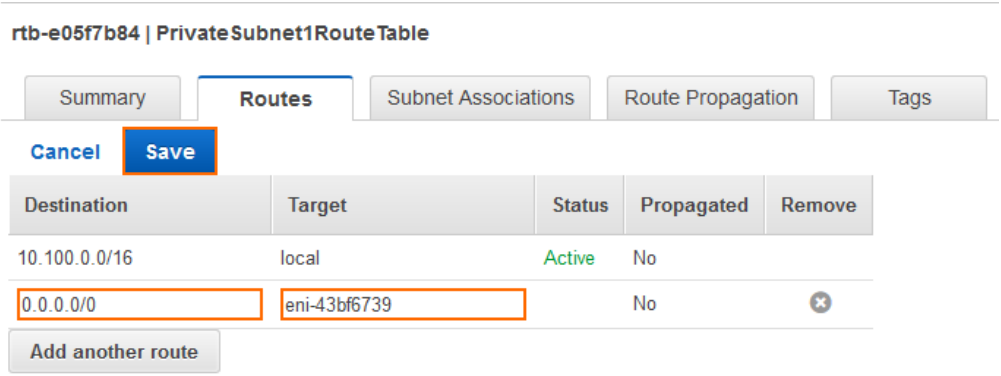
Locate the elastic network interface identifier (eni-12345678) for the network interface in this subnet. Click on the network interface in the **Description** tab of the firewall instance to retrieve the ID.



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**.

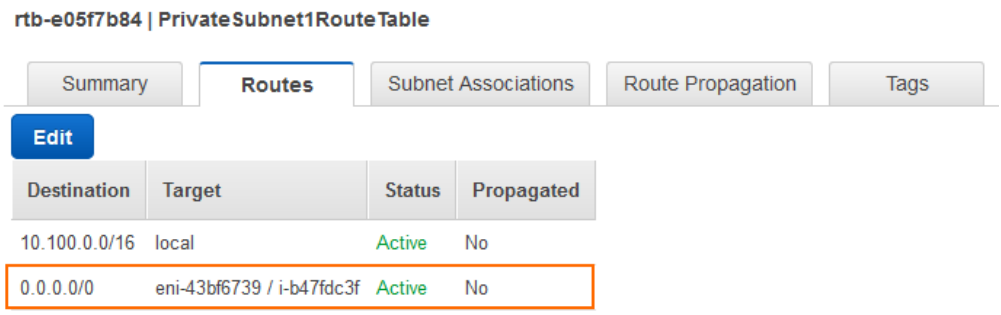


7. Click **Add another route**.
8. Configure the route:
   - **Destination** – Enter `0.0.0.0/0`.
   - **Target** – Enter the ID for the firewall network interface located in this subnet.



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**.



Figures