How to Add AWS Elastic Network Interfaces to a Firewall Instance

https://campus.barracuda.com/doc/79462723/

To make traffic between subnets visible in the firewall, you must add one network interface per subnet. The number of network interfaces you can add to your instance is limited by the instance type. Firewall instances with multiple network interfaces cannot be deployed in a high availability configuration.

AWS Reference Architectures

This article is used in the following AWS reference architectures:

- AWS Reference Architecture - Segmentation Firewall for Single AZ VPCs.

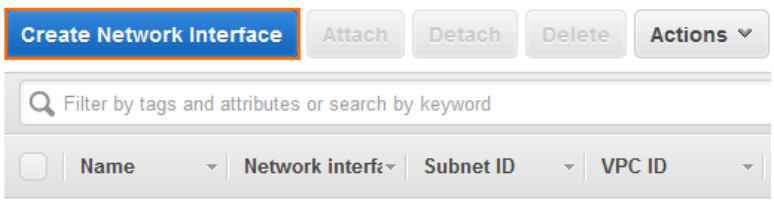
Before You Begin

- Deploy a firewall instance in the public subnet of the VPC. For more information, see How to Deploy a CloudGen Firewall in AWS via AWS Console.
- Verify that the Elastic IP address is associated with the elastic network interface (ENI) of the firewall instance and not with the instance itself.
- Stop the firewall instance. Additional network interfaces cannot be attached to a running system.

Step 1. Add an Elastic Network Interface

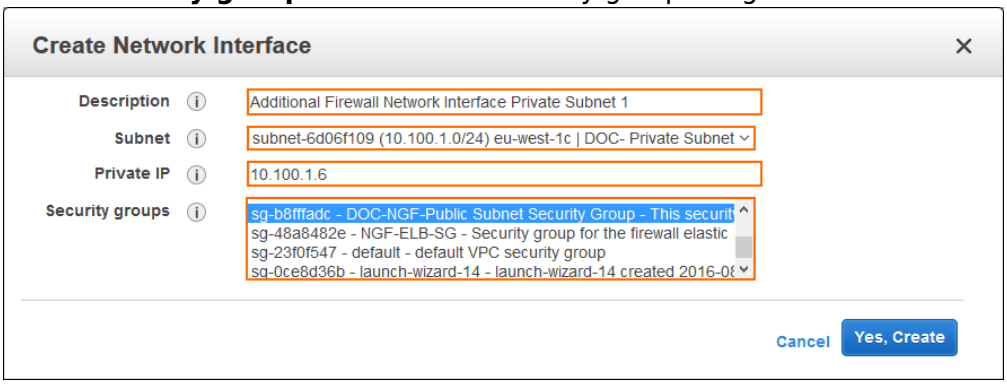
Create an elastic network interface. This interface will then be attached to the instance later.

1. Log into the AWS console.
2. Click **Services** and select **EC2**.
3. In the **Network & Services** section of the left menu, click **Network Interfaces**.
4. Click **Create Network Interface**. The **Create Network Interface** popover opens.



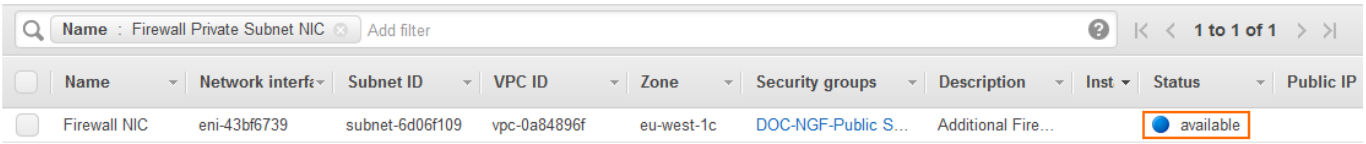
5. Configure the network interface:
   - **Description** – Enter a description for the network interface.

- **Subnet** – Select the private subnet in the VPC for the network interface. The subnet must be in the same Availability Zone as the firewall instance.
- **Private IP** – Enter a free IP address in the subnet. The first three IP addresses in the subnet are reserved by AWS.
- **Security groups** – Select the security group assigned to the firewall instance.



6. Click **Yes, Create**.

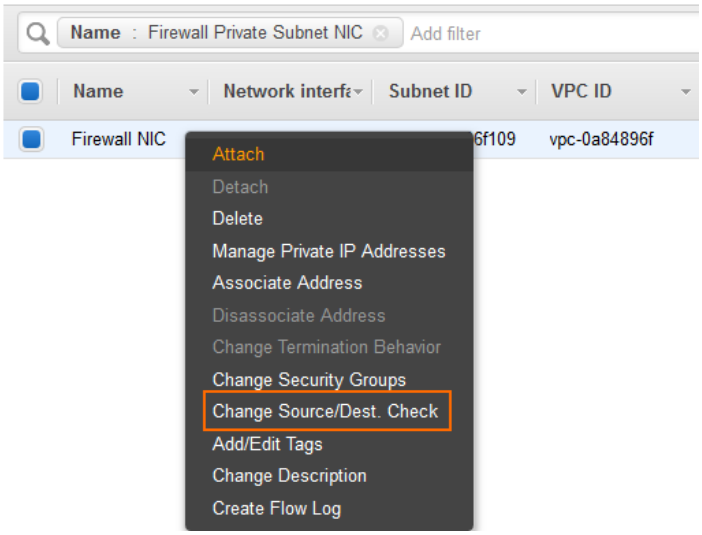
The elastic network interface is now listed with the **Status** column showing **Available**.



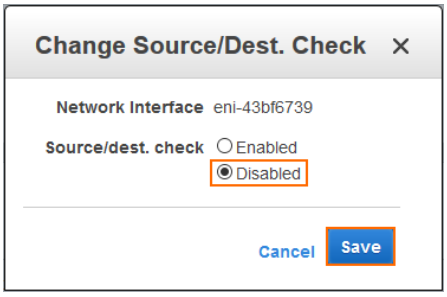
Step 2. Disable Source/Destination Check

To be able to perform NAT operations, the source/destination check must be disabled.

1. Log into the AWS console.
2. Click **Services** and select **EC2**.
3. In the **Network & Services** section of the left menu, click **Network Interfaces**.
4. Right-click on the network interface created in step 1 and click **Change Source/Dest. Check**. The **Change Source/Dest. Check** popover opens.



5. Select **Disabled**.
6. Click **Save**.

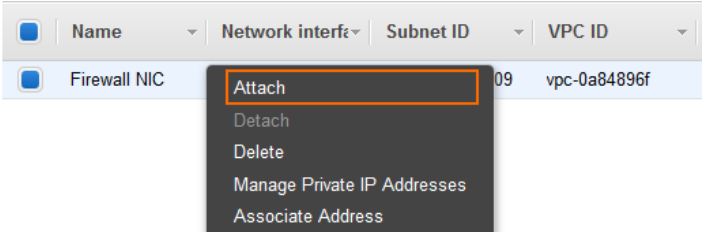


The network interface is now able to handle traffic with destination IP addresses that do not match its own private IP address.

Step 4. Attach the Network Instance to the Firewall Instance

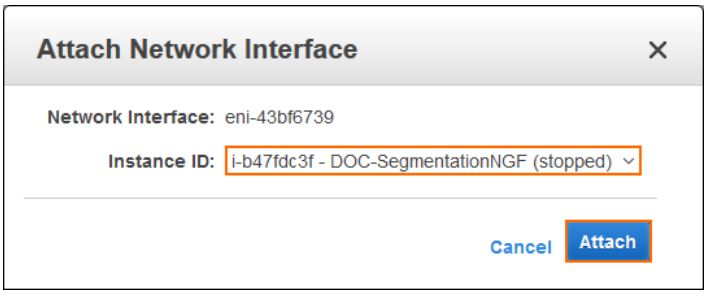
Verify that the firewall instance is shut down, and then add the network interface to the instance.

1. Log into the AWS console.
2. Click **Services** and select **EC2**.
3. In the **Network & Services** section of the left menu, click **Network Interfaces**.
4. Right-click on the network interface created in step 1 and click **Attach**. The **Attach Network Interface** popover opens.



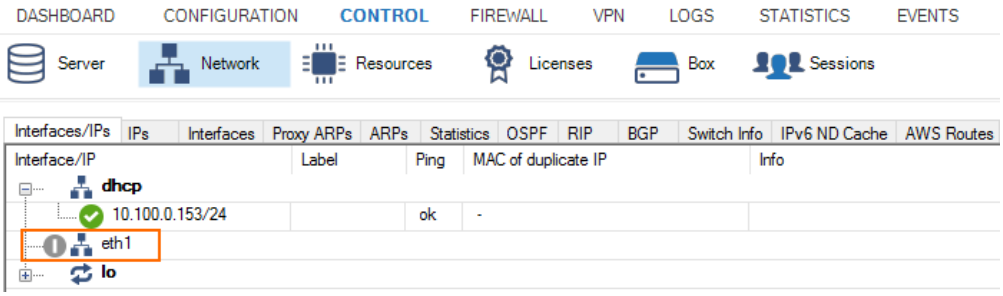
5. In the **Instance ID** list, select the firewall instance.

6. Click **Attach**.



Step 5. Start the Firewall Instance

1. Log into the AWS console.
2. Click **Services** and select **EC2**.
3. In the **Instances** section of the left menu, click **Instances**.
4. Right-click the firewall instance, select **Instance State**, and click **Start**. Wait for the firewall instance to start.
5. Log into the firewall.
6. Go to **CONTROL > Networking**.
7. Verify that the network interface you attached in step 4 is listed.

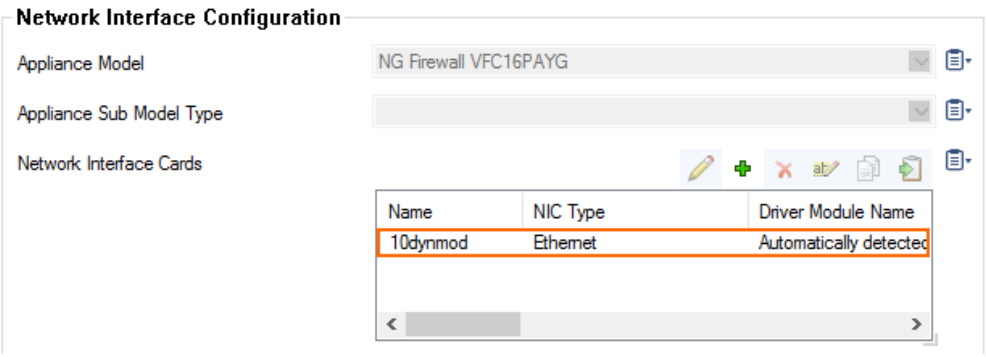


Step 6. Add the Network Interface in the Firewall Configuration

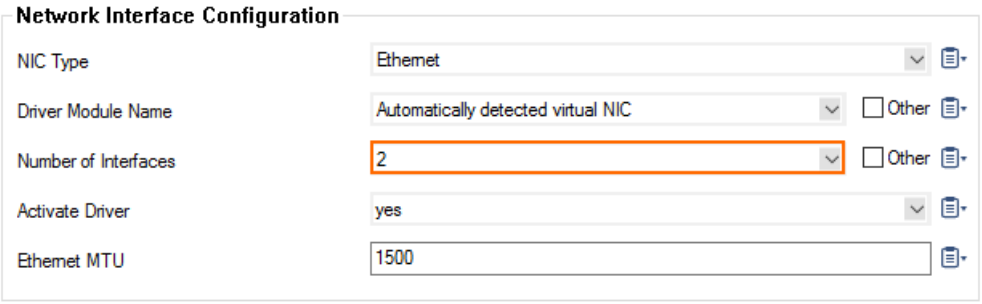
The network interface must be added and configured in the firewall configuration.

Step 6.1. Add the Network Interface

1. Log into the firewall.
2. Go to **CONFIGURATION > Configuration Tree > Box > Network**.
3. Click **Lock**.
4. In the left menu, click **Interfaces**.
5. In the **Network Interface Cards** table, double-click the **10dynmod** entry. The **Network Interface Cards: 10dynmod** window opens.



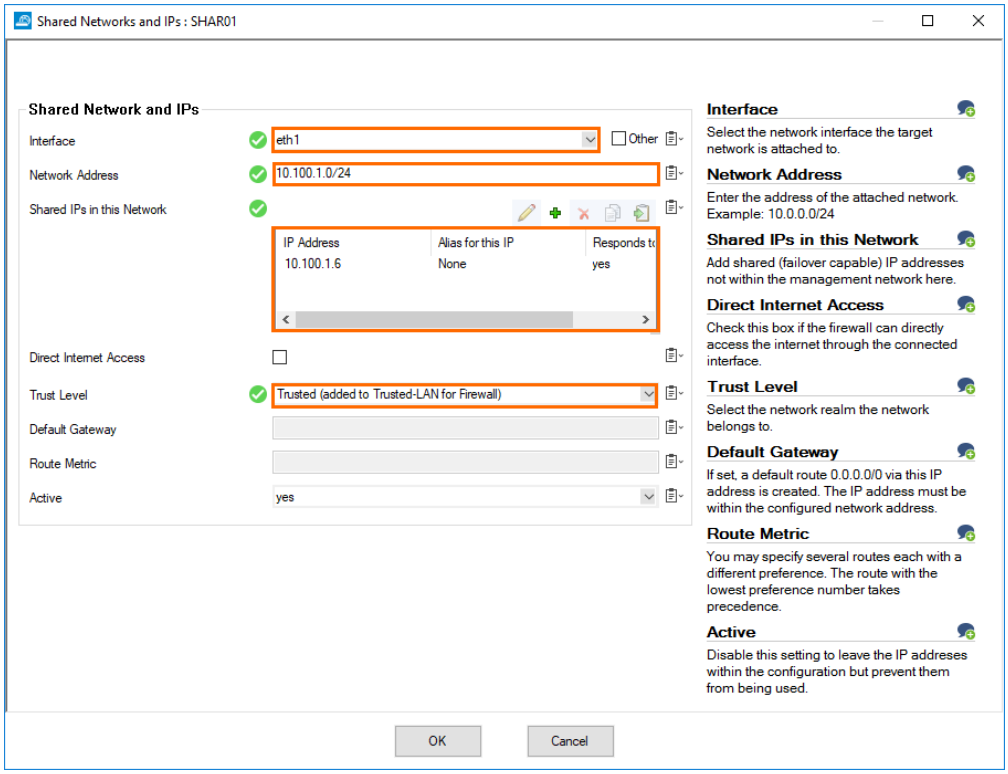
6. From the **Number of Interfaces**, select the number of network interfaces attached to the firewall instance.
7. Click **OK**.



8. Click **Send Changes** and **Activate**.

Step 6.2. Add a Shared IP for the Network Interface

1. Go to **CONFIGURATION > Configuration Tree > Box > Network**.
2. Click **Lock**.
3. In the left menu, click **IP Configuration**.
4. In the **Shared Networks and IPs** section, click **+**.
5. Enter a name for the shared IP address, and click **OK...**.
6. The **Shared Networks and IPs** window opens.
   - **Interface –** Select the interface used to connect to the network. E.g, **eth1**.
   - **Network Address** – Enter the network of the subnet in CIDR format.
   - **Shared IPs in the Network** – The **Shared IPs in this Network** window opens.
     - **IP Address** – Enter the private IP address configured for the network interface in Step 1.
     - **Alias for this IP** – Select **None**.
     - **Responds to Ping** – Select **yes** .
     - Click **OK** to save this settings.
   - **Trust Level** – Select **Trusted**.



7. Click **OK**.
8. Click **Send Changes** and **Activate**.

Step 6.3 Activate the Network Configuration

1. Go to **CONTROL > Box**.
2. In the **Network** section of the left menu, click **Activate new network configuration**. The **Network Activation** window opens.
3. Click **Failsafe**.

The route is now active and the shared IP is reachable for all clients in the subnet.

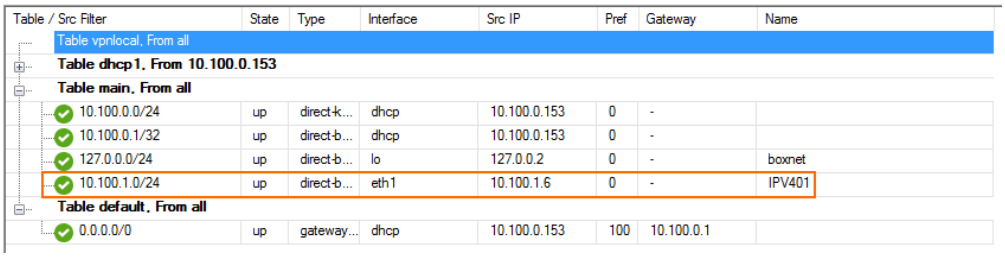


Table / Src Filter	State	Type	Interface	Src IP	Pref	Gateway	Name
Table vpnlocal, From all							
Table dhcp1, From 10.100.0.153							
Table main, From all							
10.100.0.0/24	up	direct-k...	dhcp	10.100.0.153	0	-	
10.100.0.1/32	up	direct-b...	dhcp	10.100.0.153	0	-	
127.0.0.0/24	up	direct-b...	lo	127.0.0.2	0	-	boxnet
10.100.1.0/24	up	direct-b...	eth1	10.100.1.6	0	-	IPV401
Table default, From all							
0.0.0.0/0	up	gateway...	dhcp	10.100.0.153	100	10.100.0.1	

Next Steps

- Configure the AWS route table to use the network interface as the default route for all clients in this subnet.

- To send traffic between two subnets over the firewall, the firewall must have a network interface in each subnet. A gateway route must be added on the clients with the private IP address of the firewall used as the gateway. For more information, see AWS Reference Architecture - Segmentation Firewall for Single AZ VPCs.

Figures

1. add_eni_01.png
2. add_eni_02.png
3. add_eni_03.png
4. add_eni_04.png
5. add_eni_05.png
6. add_eni_06.png
7. add_eni_07.png
8. add_eni_08.png
9. add_eni_09.png
10. add_eni_10.png
11. shared_networks_and_ips.png
12. add_eni_14.png