

## How to Add AWS Elastic Network Interfaces to a Firewall Instance

<https://campus.barracuda.com/doc/54263910/>

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.](#)

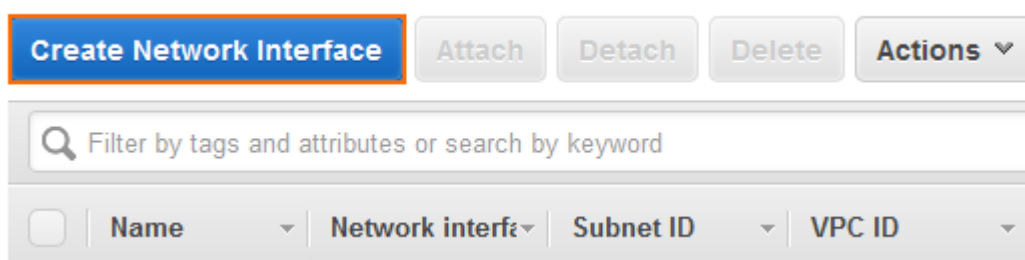
### Before You Begin

- Deploy a firewall instance in the public subnet of the VPC. For more information, see [How to Deploy an F-Series Firewall in AWS via Web Portal.](#)
- 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

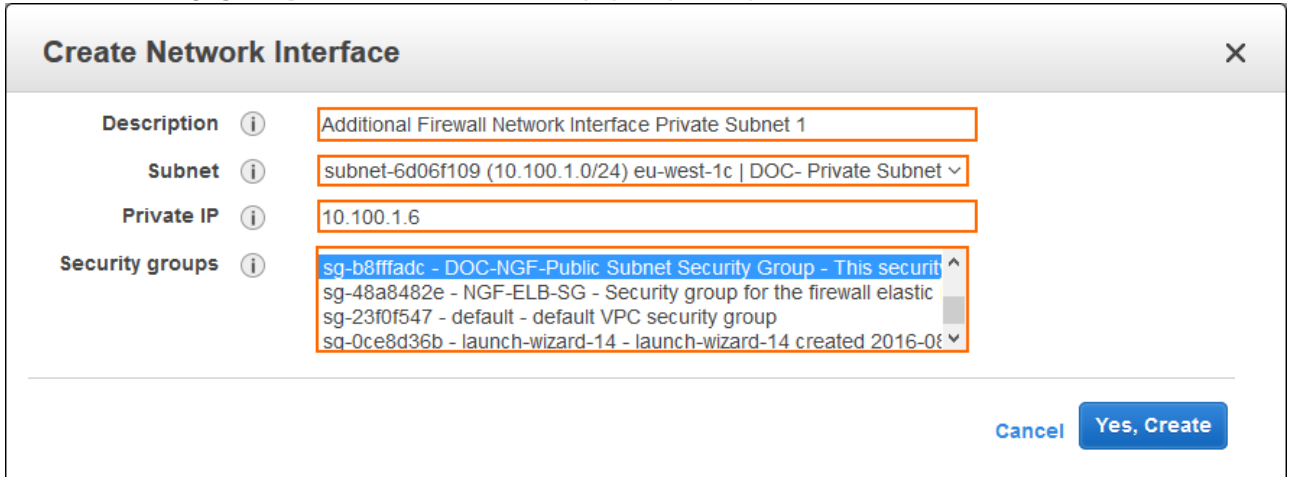
Create an elastic network interface. This interface will then be attached to the instance later.

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**.

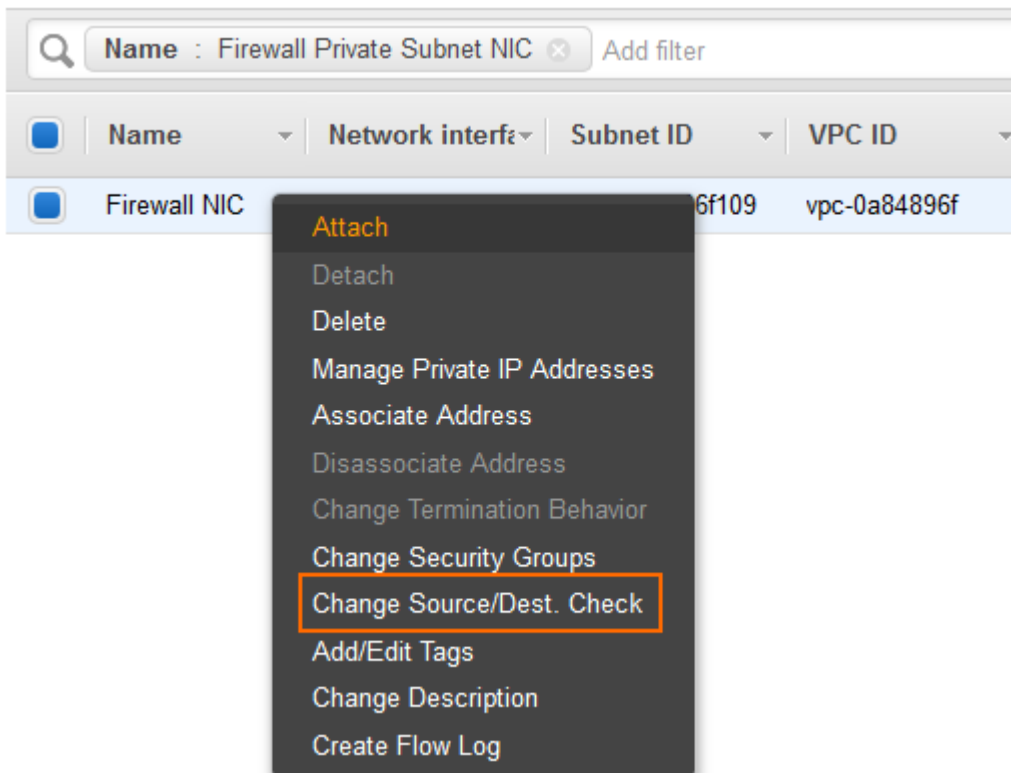
The elastic network interface is now listed with the **Status** column showing **Available**.

Name	Network interface	Subnet ID	VPC ID	Zone	Security groups	Description	Inst	Status	Public IP
Firewall NIC	eni-43bf6739	subnet-6d06f109	vpc-0a84896f	eu-west-1c	DOC-NGF-Public S...	Additional Fire...		available	

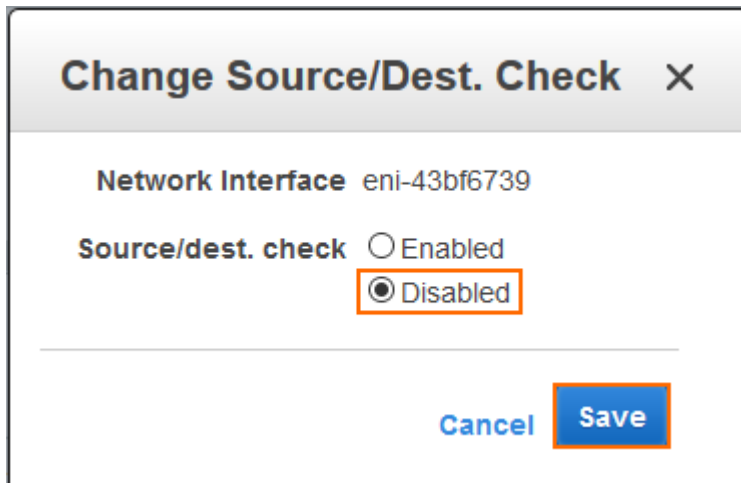
## Step 2. Disable Source/Destination Check

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**.

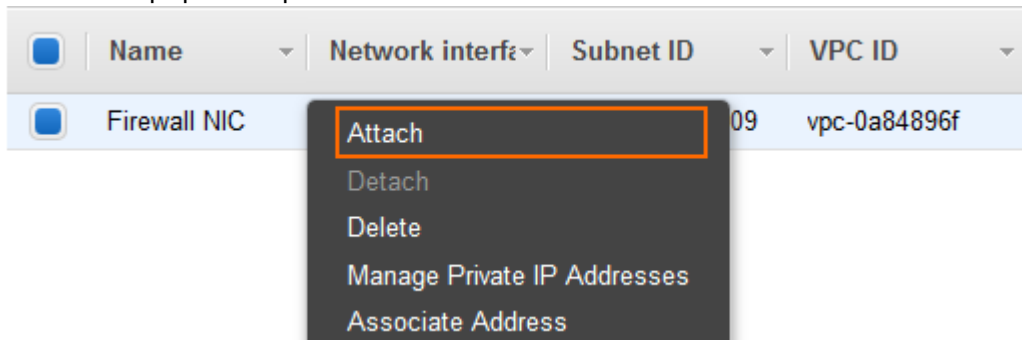


The network interface is now able to handle traffic with destination IP addresses that do not match its own private IP address.

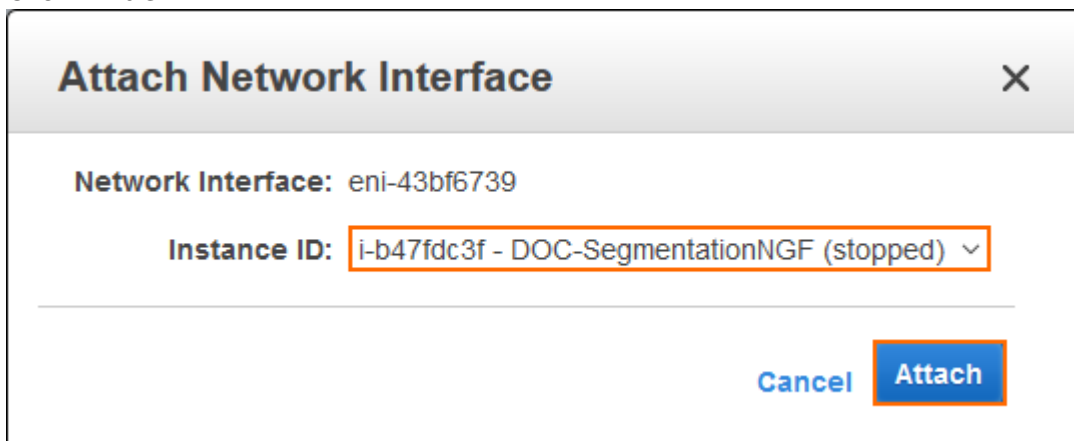
#### Step 4. Attach the Network Instance to the Firewall Instance

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.

DASHBOARD   CONFIGURATION   **CONTROL**   FIREWALL   VPN   LOGS   STATISTICS   EVENTS

Server   **Network**   Resources   Licenses   Box   Sessions

Interfaces/IPs	IPs	Interfaces	Proxy ARPs	ARPs	Statistics	OSPF	RIP	BGP	Switch Info	IPv6 ND Cache	AWS Routes
Interface/IP		Label		Ping	MAC of duplicate IP						Info
dhcp	10.100.0.153/24			ok	-						
eth1											
lo											

## 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.

**Network Interface Configuration**

Appliance Model: NG Firewall VFC16PAYG

Appliance Sub Model Type:

Network Interface Cards

Name	NIC Type	Driver Module Name
10dynmod	Ethernet	Automatically detected

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

Network Interface Configuration	
NIC Type	Ethernet <input type="button" value="copy"/>
Driver Module Name	Automatically detected virtual NIC <input type="checkbox"/> Other <input type="button" value="copy"/>
Number of Interfaces	2 <input type="checkbox"/> Other <input type="button" value="copy"/>
Activate Driver	yes <input type="button" value="copy"/>
Ethernet MTU	1500 <input type="button" value="copy"/>

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

### Step 6.2. Add a Direct Attached Route for the Network Interface

Add the subnet the network interface is in as a direct attached route.

1. Go to **CONFIGURATION > Configuration Tree > Box > Network**.
2. Click **Lock**.
3. In the left menu, click **Routing**.
4. Click **+** in the **IPv4 Routing Table** to add an attached route.
  - **Target Network Address** - Enter the network of the subnet in CIDR format.
  - **Route Type** - Select **direct attached network**.
  - **Interface Name** - Select the interface used to connect to the network. E.g, **eth1**
  - **Trust Level** - Select **Trusted**.

Route Configuration	
Target Network Address	10.100.1.0/24 <input type="button" value="copy"/>
Route Type	directly attached network <input type="button" value="copy"/>
Interface Name	eth1 <input type="checkbox"/> Other <input type="button" value="copy"/>
Gateway	<input type="button" value="copy"/>
Route Metric	<input type="button" value="copy"/>
Source Address	<input type="button" value="copy"/>
Trust Level	Trusted (added to Trusted-LAN for Firewall) <input type="button" value="copy"/>
Default Gateway	<input type="button" value="copy"/>
Route Origin	User created <input type="button" value="copy"/>
Active	yes <input type="button" value="copy"/>

5. Click **OK**.
6. Click **Send Changes** and **Activate**.

### Step 6.4 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 pending in **CONTROL > Network**.

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							
<input checked="" type="checkbox"/> 10.100.0.0/24	up	direct-k...	dhcp	10.100.0.153	0	-	
<input checked="" type="checkbox"/> 10.100.0.1/32	up	direct-b...	dhcp	10.100.0.153	0	-	
<input checked="" type="checkbox"/> 127.0.0.0/24	up	direct-b...	lo	127.0.0.2	0	-	boxnet
<input checked="" type="checkbox"/> 10.100.1.0/24	off	direct	eth1	-	0	-	IPV401
Table default, From all							
<input checked="" type="checkbox"/> 0.0.0.0/0	up	gateway...	dhcp	10.100.0.153	100	10.100.0.1	

### Step 6.3 Add a Virtual Server IP

Add the private IP address assigned to the network interface as a virtual server IP address.

1. Go to **CONFIGURATION > Configuration Tree > Box > Virtual Servers > your virtual server > Server Properties**.
2. Click **Lock**.
3. Click **+** in the **Additional IP** table. The **Additional IP** window opens.
4. Configure the additional virtual server IP:
  - **Additional IP** - Enter the private IP address configured for the network interface in step 1.
  - **Reply to Ping** - Select **yes**.

Additional IP	<input type="text" value="10.100.1.6"/>	
Label	<input type="text"/>	
Reply to Ping	<input type="text" value="yes"/>	
Description	<input type="text"/>	

5. Click **OK**.
6. Click **Send Changes** and **Activate**.

The route is now active and the virtual server IP 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. add\_eni\_11.png
12. add\_eni\_12.png
13. add\_eni\_13.png
14. add\_eni\_14.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.