How to Deploy the Barracuda NG Firewall in an Amazon Virtual Private Cloud

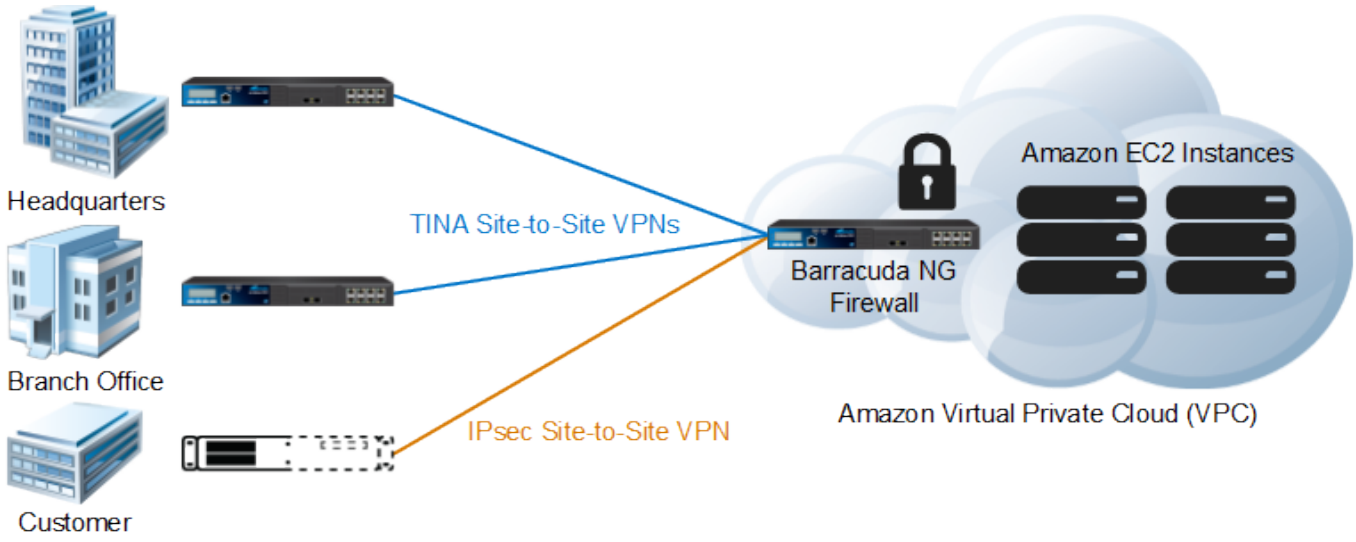
https://campus.barracuda.com/doc/41115872/

The Barracuda NG Firewall 6.0 image is no longer available in the AWS marketplace. Use the newest available NextGen Firewall F-Series image instead. For more information, see Amazon AWS Deployment.

The Barracuda NG Firewall can run as a virtual appliance in the Amazon cloud as a gateway device for Amazon EC2 instances in an Amazon Virtual Private Cloud (VPC).

Follow the steps in this article to deploy the Barracuda NG Firewall in an Amazon VPC.

Amazon AWS charges apply. For more information, see Amazon's monthly pricing calculator at http://calculator.s3.amazonaws.com/calc5.html.



In this article:

Before you Begin

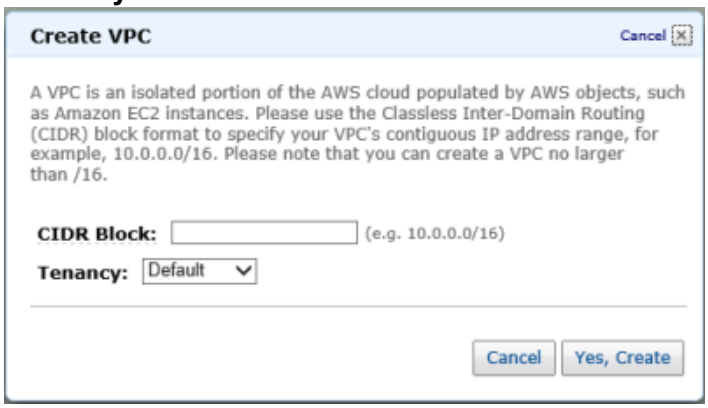
Before you deploy the Barracuda NG Firewall in the Amazon VPC:

- Get an Amazon Web Service (AWS) account.
- Get a Barracuda NG Firewall Vx license. The Barracuda NG Firewall AMI itself is free (BYOL = Bring Your Own License).
- Choose the country and availability zone in which you want to create the Amazon VPC. All instances and services must be in the same availability zone.

Step 1. Set Up the Amazon VPC Cloud

The Amazon VPC is a smaller, isolated version of the public Amazon Elastic Compute Cloud (EC2). The VPC is restricted to its own /16 network subnet. Create a VPC in the 192.168.0.0/16 subnet.

1. Go to the Amazon Web Services Console (https://console.aws.amazon.com).
2. In the **Compute & Networking** section, click **VPC - Isolated Cloud Resources**.
3. In the left pane of the VPC console, click **Your VPCs**.
4. Create a VPC with the following settings:
   - **CIDR Block** – Enter `192.168.0.0/16`.
   - **Tenancy** – Select **Default**.



5. Click **Yes, Create**.

Your VPC is now listed on the **Your VPCs** page.

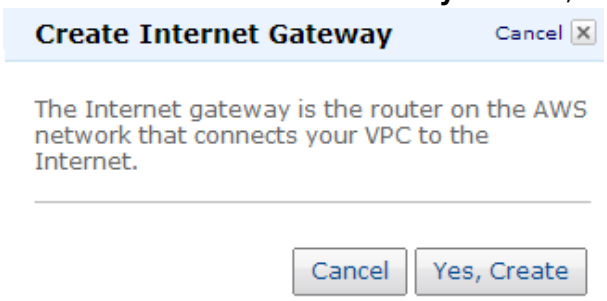
	VPC ID	State	CIDR	DHCP Options Set	Main Route Table	Default Network ACL	Tenancy	Default VPC
☑	vpc-b0a9a0db	available	192.168.0.0/16	dopt-b4a9a0df	rtb-b6a9a0dd	acl-b7a9a0dc	default	false

Step 2. Create an Internet Gateway

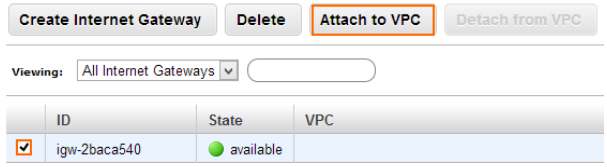
Create an Internet gateway to enable devices in the Amazon VPC to access the Internet.

1. Go to the Amazon Web Services VPC console (https://console.aws.amazon.com/vpc/home).

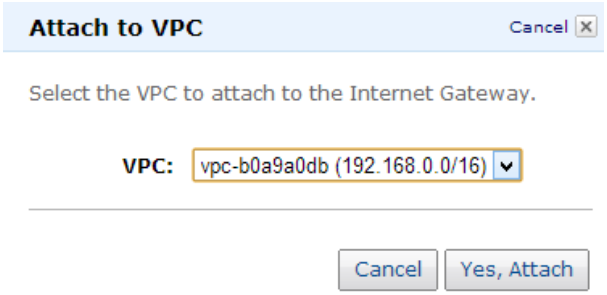
2. In the left pane, click **Internet Gateways**.
3. Click **Create Internet Gateway**.
4. In the **Create Internet Gateway** window, click **Yes, Create**.



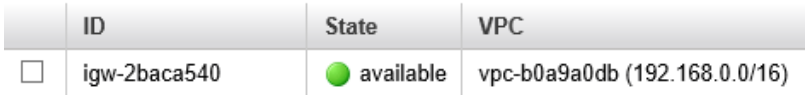
5. Select the new Internet gateway, and then click **Attach to VPC**.



6. Select the VPC that you created in Step 1 (e.g., **vpc-b0a9a0db (192.168.0.0/16)**), and then click **Yes, Attach**.



The Internet gateway is now associated with the Amazon VPC.



Step 3. Create Subnets

Create two /24 subnets inside the Amazon VPC:

- A public network that connects the dhcp (eth0) interface of the Barracuda NG Firewall to the Internet gateway.
- A private network for the eth1 interface on the Barracuda NG Firewall and the EC2 instances in the VPC.

Step 3.1. Create the Private Subnet

1. Go to the Amazon Web Services VPC console (https://console.aws.amazon.com/vpc/home).
2. In the left pane, click **Subnets**.
3. Click **Create Subnet**.
4. In the **Create Subnet** window, configure the following settings:
   - **VPC** – Select the VPC with the 192.168.0.0./16 subnet (e.g., **vpc-abcd1234568 (192.168.0.0/16)**).
   - **Availability Zone** – Select the availability zone that your VPC is in (e.g., **eu-west-1a**).
   - **CIDR Block** – Enter `192.168.200.0/24`.
5. Click **Yes, Create**.

Step 3.2. Create the Public Subnet

1. Go to the Amazon Web Services VPC console (https://console.aws.amazon.com/vpc/home).
2. Click **Subnets**.
3. Click **Create Subnet**.
4. In the **Create Subnet** window, configure the following settings:
   - **VPC** – Select the VPC with the 192.168.0.0./16 subnet (e.g., **vpc-abcd1234568 (192.168.0.0/16)**).
   - **Availability Zone** – Select the availability zone that your VPC is in (e.g., **eu-west-1a**).
   - **CIDR Block** – Enter any 192.168.*XX*.0/24 subnet, except for 192.168.200.0/24 (e.g., you can enter `192.168.10.0/24`).
5. Click **Yes, Create**.

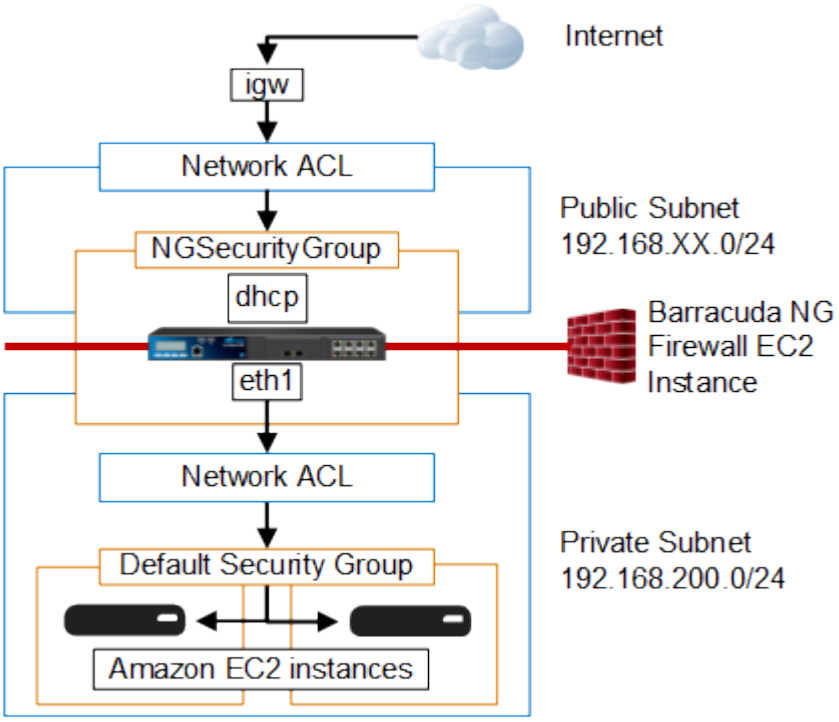
The private (192.168.200.0/24) and public (192.168.10.0/24) subnets are now in your VPN.

	Subnet ID	State	VPC ID	CIDR	Available IPs	Availability Zone	Route Table	Network ACL	Default Subnet
☐	subnet-e8a8a183	available	vpc-b0a9a0db	192.168.200.0/24	251	eu-west-1a	rtb-b6a9a0dd	Default	false
☐	subnet-f6a8a19d	available	vpc-b0a9a0db	192.168.10.0/24	251	eu-west-1a	rtb-b6a9a0dd	Default	false

Step 4. Set Up Amazon Security Groups and Network ACLs

To secure incoming and outgoing connections to the VPC, set up the following features:

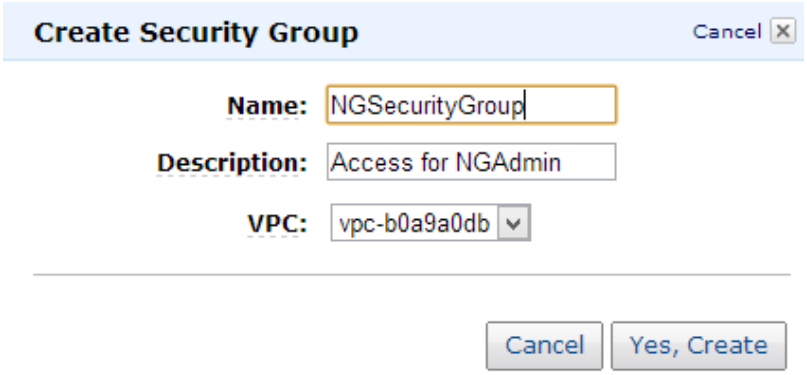
- **Security Groups** – Act as stateful firewalls that control traffic to one or more Amazon EC2 instances. Every instance must be associated with one or more security groups. With security groups, you can only allow specific connections; by default, connections are blocked.
- **Network ACLs** – Act as a stateless firewall that controls traffic going in and out of a subnet. With network ACLs, you can allow and block connections. By default, an Amazon network ACL blocks all traffic.



For more information on Amazon security groups and network ACLs, see http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Security.html.

Step 4.1. Create a Security Group for Barracuda NG Admin Access

1. Go to the Amazon Web Services VPC console (https://console.aws.amazon.com/vpc/home).
2. In the left pane, expand **SECURITY** and then click **Security Groups**.
3. Click **Create Security Group**.
4. In the **Create Security Group** window, configure the following settings:
   - **Name** – Enter `NGSecurityGroup`.
   - **Description** – Enter `Access for NG Admin`.
   - **VPC** – Select the VPC from the list (e.g., **vpc-b0a9a0db**).
5. Click **Yes, Create**.



6. Select **NGSecurityGroup**.
7. In the lower pane, click the **Inbound** tab.
8. Add rules with the following settings to allow inbound traffic for the SSH daemon and ping:

Create a new Rule	Source

SSH	0.0.0.0/0
All ICMP	0.0.0.0/0
DNS	0.0.0.0/0

9. Add custom rules with the following settings to allow inbound traffic for Barracuda NG Admin (port 807), the VPN service (port 691), and the management tunnel (port 692):

Create a new Rule	Port range	Source
Custom TCP rule	807	0.0.0.0/0
Custom UDP rule	807	0.0.0.0/0
Custom TCP rule	691-692	0.0.0.0/0
Custom UDP rule	691-692	0.0.0.0/0

10. Create additional rules for all services running on the Barracuda NG Firewall and all services forwarded for EC2 Instances in the Amazon VPC (e.g., port 80/443 for web servers, port 25 for SMTP, etc.).
11. Click **Apply Rule Changes**.

All inbound rules are now listed under the **Inbound** tab of the security group.

Step 4.2. Configure a Security Group for the Private Subnetwork

Instances in the private subnetwork are only accessed by connections passing through the Barracuda NG Firewall EC2 instance. Configure the default security group to only allow traffic that is coming from the NGSecurityGroup.

1. Go to the Amazon Web Services VPC console (https://console.aws.amazon.com/vpc/home).
2. In the left pane, expand **SECURITY** and then click **Security Groups**.
3. Select the **default** security group.
4. In the lower pane, click the **Inbound** tab.
5. Add rules with the following settings to allow incoming traffic for the default security group coming from the NGSecurityGroup and for traffic within in the default security group.

Rule	Rule Settings
To allow incoming traffic from the NGSecurityGroup.	◦ **Create a new Rule** – Select **All Traffic**. ◦ **Source** – Enter the group ID for NGSecurityGroup (e.g., sg-cf49bca0). You can find the group ID by selecting the NGSecurityGroup security group and then clicking the **Details** tab.
To allow incoming traffic from the default security group.	◦ **Create a new Rule** – Select **All Traffic**. ◦ **Source** – Enter the group ID for the default security group (e.g., sg-ae4ebbc1). You can find the group ID by selecting the default security group and then clicking the **Details** tab.

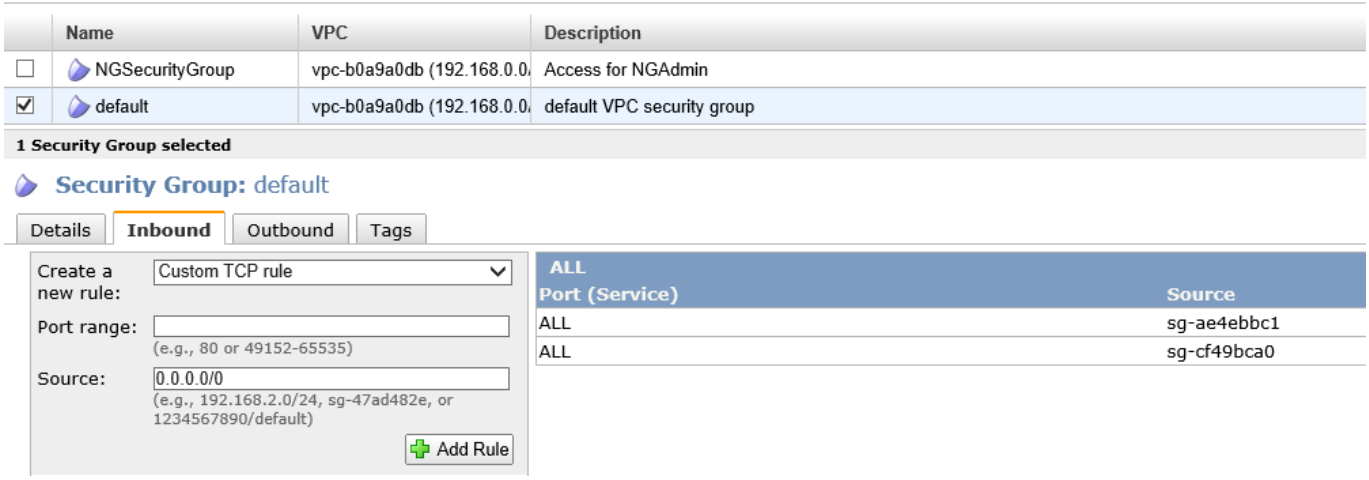
6. Click **Apply Rule Changes**.
7. Click the **Outbound** tab.
8. Add the following rules to allow all outgoing traffic coming from the default security group going

to the NGSecurityGroup or for traffic within the default security group.

Rule	Rule Settings
To allow outgoing traffic to the NGSecurityGroup.	◦ **Create a new Rule** – Select **All Traffic**. ◦ **Source** – Enter the group ID for NGSecurityGroup (e.g., `sg-cf49bca0`). You can find the group ID by selecting the NGSecurityGroup security group and then clicking the **Details** tab.
To allow outgoing traffic within the default security group.	◦ **Create a new Rule** – Select **All Traffic**. ◦ **Source** – Enter the group ID for the default security group (e.g., `sg-ae4ebbc1`). You can find the group ID by selecting the default security group and then clicking the **Details** tab.

9. Click **Apply Rule Changes**.

The default security group now lets all traffic pass between the two security groups.



Step 4.3. Set Up the Network ACLs

By default, network ACLs block all incoming and outgoing traffic. To use the Barracuda NG Firewall instead of the Amazon network ACL, add rules to allow all inbound and outbound traffic.

To use the Barracuda NG Firewall as a gateway device, allow all traffic into the private network.

1. Go to the Amazon Web Services VPC console (https://console.aws.amazon.com/vpc/home).
2. In the left pane, expand **SECURITY** and then click **Network ACLs**.
3. Click **Create Network ACL**.
4. Select the **VPC** with the 192.168.0.0./16 subnet (e.g., **vpc-abcd1234568 (192.168.0.0/16)**), and then click **Yes, Create**.
5. Click the **Inbound** tab.
6. Add a rule with the following settings to allow inbound traffic.

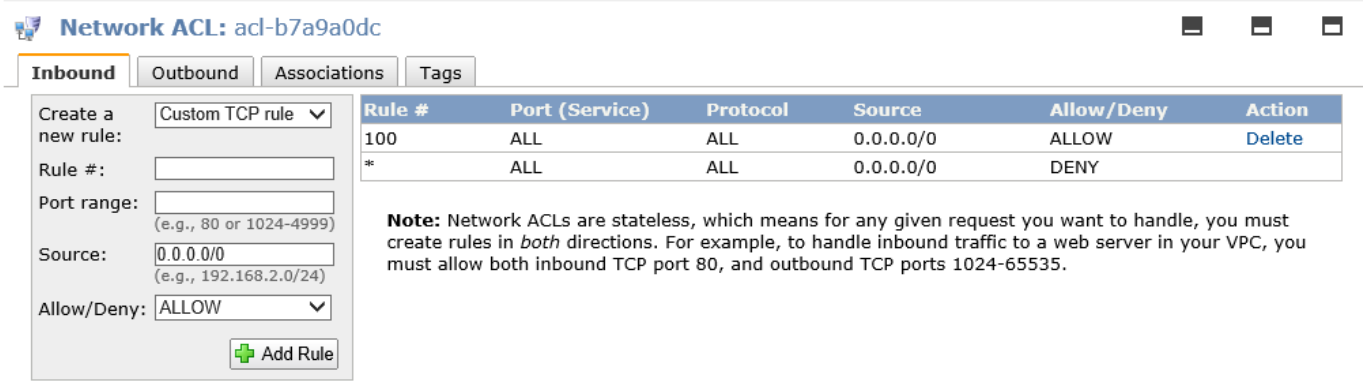
Traffic	Rule Settings

Inbound	◦ **Create a new Rule**: **All Traffic** ◦ **Rule #**: `100` ◦ **Source**: `0.0.0.0/0` ◦ **Allow/Deny**: **ALLOW**

7. Click the **Outbound** tab.
8. Add a rule with the following settings to allow outbound traffic.

Traffic	Rule Settings
Outbound	◦ **Create a new Rule**: **All Traffic** ◦ **Rule #**: `100` ◦ **Source**: `0.0.0.0/0` ◦ **Allow/Deny**: **ALLOW**

The network ACL now permits all traffic on all ports in and out of the subnets. All hosts in the private network are protected by the Firewall service running on the Barracuda NG Firewall.



Step 5. Deploy a Barracuda NG Firewall in an Amazon EC2 Instance

In the Amazon VPC that you created in Step 1, launch an Amazon EC2 instance with the Barracuda NG Firewall AMI image. Note that the Barracuda NG Firewall AMI image is EBS backed, so powering down the Barracuda NG Firewall EC2 instance will not result in data loss. The Barracuda NG Firewall will be launched with one dynamic DHCP interface. More Network interfaces are added after launching the Instance. The **Amazon Launch Instance** wizard guides you through the following steps:

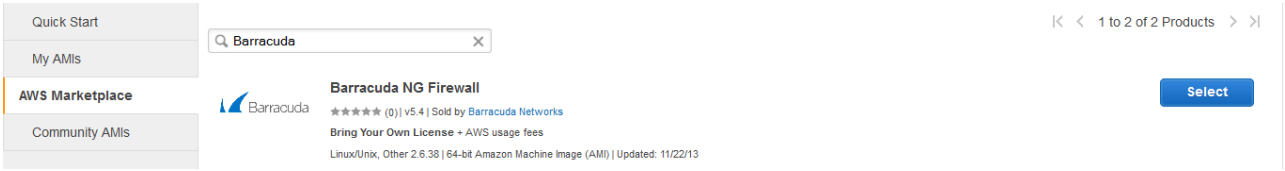
Start the Amazon Launch Instance Wizard

1. Go to the Amazon Web Services EC2 console (https://console.aws.amazon.com/ec2/home).
2. Click **Launch Instance**.

Launch Instance Wizard Step 1: Choose AMI

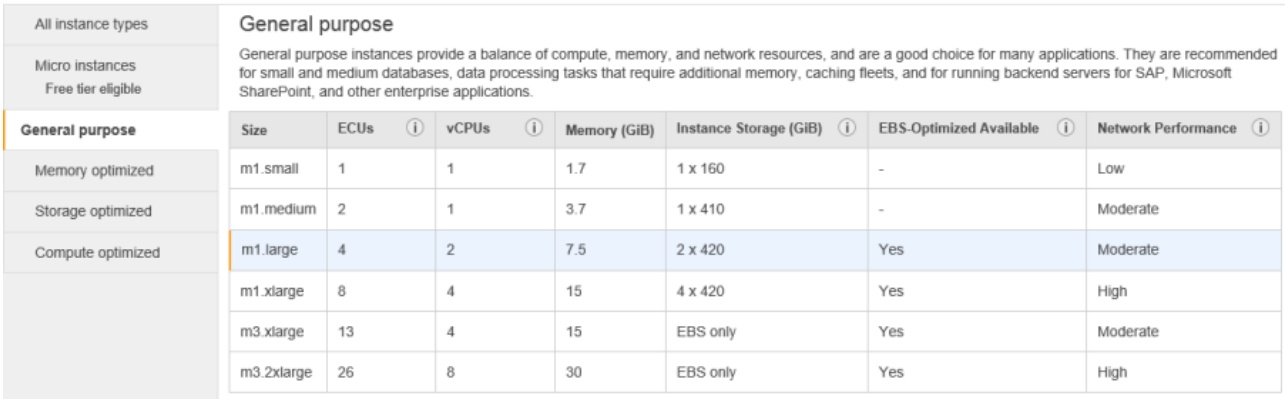
1. Click on **AWS Marketplace** in the left navigation.
2. Enter `Barracuda NG Firewall` in the search box and click **Search**.

3. Click **Select** next to the Barracuda NG Firewall image you want to install (e.g., Barracuda NG Firewall).



Launch Instance Wizard Step 2: Choose Instance Type

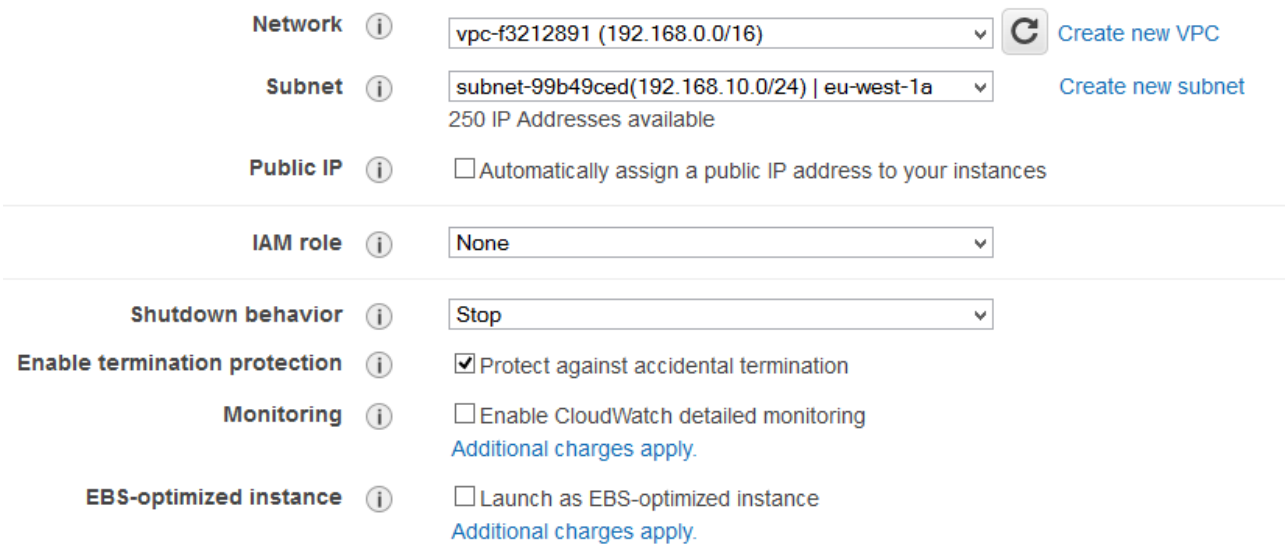
1. Select an EC2 instance type. Verify that the number of CPUs for your license matches the number of vCPUs of the EC2 instance type.



2. Click **Next: Configure Instance Details**.

Launch Instance Wizard Step 3: Configure Instance

1. From the **Network** list, select the VPC created in Step 1 (e.g., **vpc-b0a9a0db (192.168.0.0/16)**).
2. From the **Subnet** list, select the 192.168.XX.0/24 subnet created in Step 3.2 (e.g., **subnet-f6a8a19d (192.168.10.0/24)**).
3. Select the **Enable termination protection** check box.
4. (Optional) To improve I/O performance, enable **EBS-optimized instance**.



5. Click **Next: Add Storage**.

Launch Instance Wizard Step 4: Add Storage

1. (Optional) If you want the EBS volumes to be deleted after the Barracuda NG Firewall EC2 instance has been terminated (deleted), select the **Delete on Termination** check boxes.
2. (Optional) Enter a larger **Size** for the **/dev/sdf** EBS volume.
3. (Optional) To improve the I/O performance of your EC2 instance, select **Provisioned IOPS** from the **Volume Type** list.

Type	Device	Snapshot	Size (GB)	Volume Type	IOPS	Delete on Termination
Root	/dev/sda1	snap-03faa312	10	Provisioned IOPS	300	☐
EBS	/dev/sdf	snap-a2fea7b3	80	Standard	N/A	☐

4. Click **Next: Tag Instance**.

Launch Instance Wizard Step 5: Tag Instance

1. (Optional) Add tags to identify your EC2 instance.
2. Click **Next: Configure Security Group**.

Launch Instance Wizard Step 6: Configure Security Group

1. From the **Assign a security group** list, select **Select an existing security group**.
2. Select the **NGSecurityGroup** that you created in Step 4.1 from the list of Security Group (e.g., **sg-cf49bca0- NGSecurityGroup**).

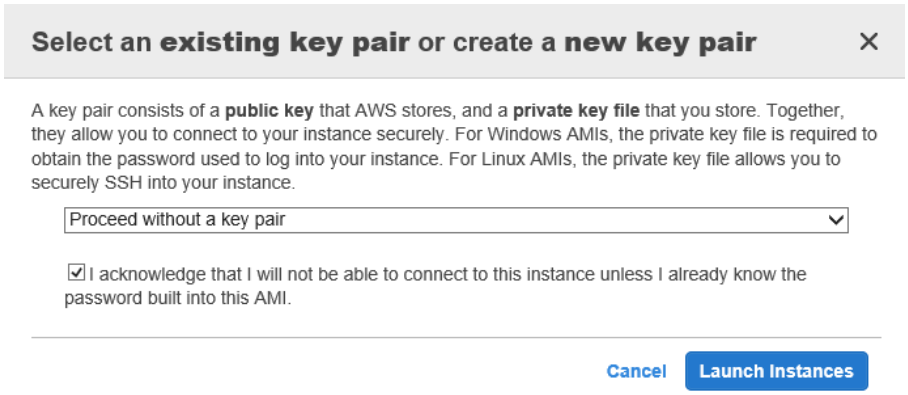
Assign a security group: ○ Create a **new** security group
● Select an **existing** security group

	Security Group ID	Name	Description
☐	sg-0b10e464	default	default VPC security group
☑	sg-7e50a411	NGSecurityGroup	Security Group NG admin

3. Click **Review and Launch**.
4. In the **Warning** window, click **Continue**.

Launch Instance Wizard Step 7: Review

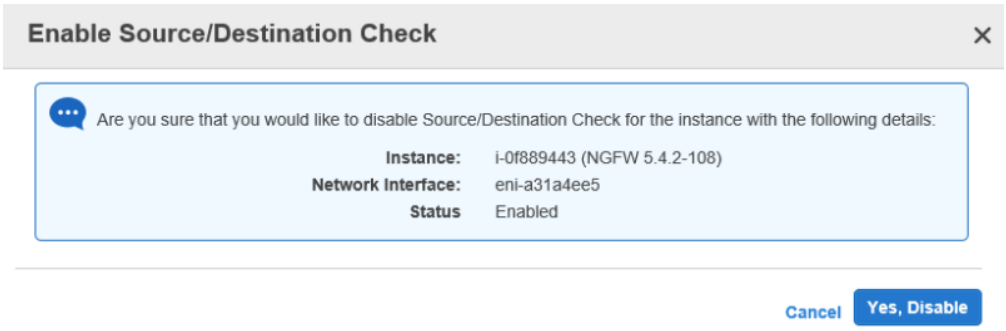
1. Click **Launch**.
2. In the **Select an existing key pair or create a new key pair** window:
   - Select **Proceed without a key pair**.
   - Click the check box to acknowledge that you will not be able to connect to this instance unless you already know the password built into the AMI.



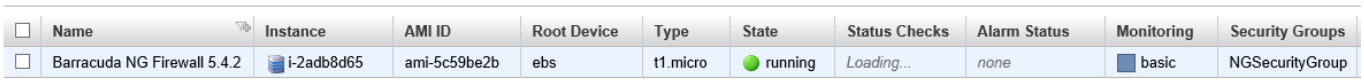
3. Click **Launch Instances**.

Deactivate the Source/Destination Check

1. Click **View Instances**.
2. Right-click the Barracuda NG EC2 instance that you just created, and then select **Change Source/Dest. Check**.
3. Click **Yes, Disable**.



Your EC2 Instance appears in the EC2 list. After the instance is up, the **State** and **Status Checks** change to green.



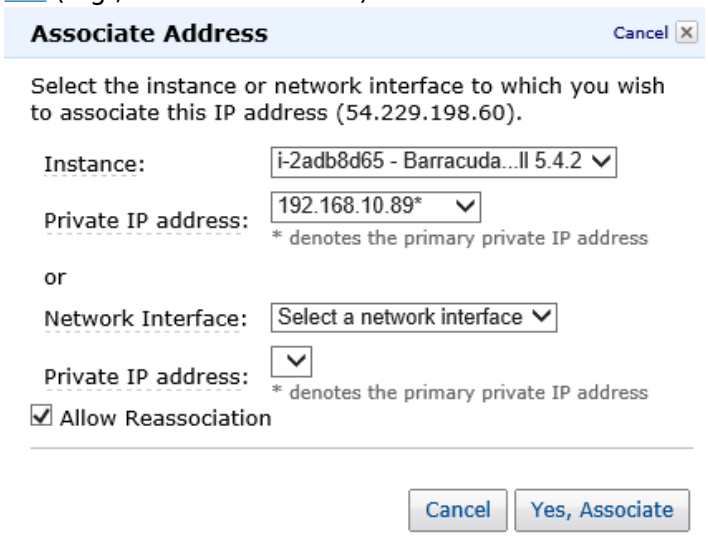
Name	Instance	AMI ID	Root Device	Type	State	Status Checks	Alarm Status	Monitoring	Security Groups
Barracuda NG Firewall 5.4.2	i-2adb8d65	ami-5c59be2b	ebs	t1.micro	running	Loading...	none	basic	NGSecurityGroup

Step 6. Allocate and Associate an Amazon Elastic IP Address to the Barracuda NG Firewall EC2 Instance

The private IP address assigned to the external interface (eth1) on the Barracuda NG Firewall instance is not yet reachable from the Internet. Create and attach an Amazon Elastic IP Address (EIP) to the external network interface.

1. Go to the Amazon Web Services VPC console (https://console.aws.amazon.com/vpc/home).
2. In the left pane, click **Elastic IPs**.

3. Click **Allocate New Address**.
4. From the **EIP used in** list, select **VPC**.
5. Click **Yes, Allocate**.
6. Select the new EIP, and then then click **Associate Address**.
7. In the **Associate Address** window, configure the following settings:
   - **Instance** – Select the Barracuda NG Firewall instance (e.g., **i-2adb8d65 (Barracuda NG Firewall 5.4.2)**).
   - **Private IP address** – Select the IP address in the public subnet that you created in Step 3.2 (e.g., **192.168.10.89***).



8. Click **Yes, Associate**.

Your EIP is now listed with the instance ID and ENI ID associated with the Barracuda NG Firewall instance.

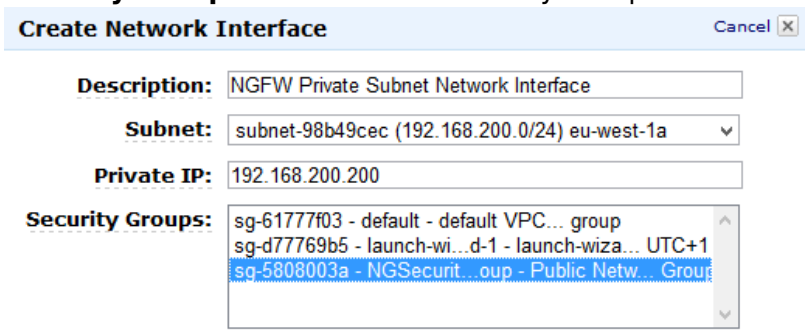
Address	Instance ID	ENI ID	Scope	Public DNS
54.229.198.60	i-2adb8d65 (Barracuda NG Firewall 5.4.2)	eni-79696112	vpc-b0a9a0db (192.168.200.0/24)	

Step 7. Create and Attach a Network Interface

Create a Network Interface in the private subnet. This interface will be registered as eth1 on the Barracuda NG Firewall.

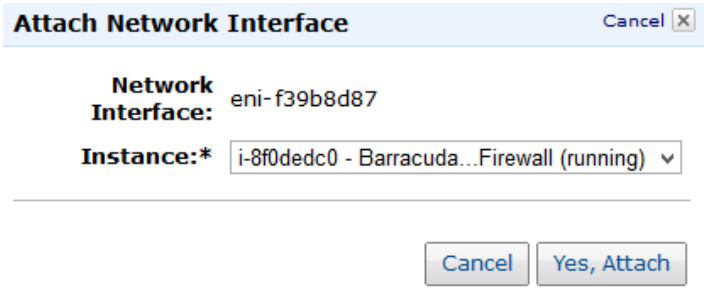
1. Go to the Amazon Web Services EC2 console (https://console.aws.amazon.com/ec2/home).
2. In the left pane, click on **Network Interfaces**.
3. Click **Create Network Interface**.
4. Configure the Network Interface with the following settings:
   - **Subnet** – Select the private subnet (**192.168.200.0/24)** you created in Step 3.1. E.g., **subnet-e8a8a183**
   - **Private IP** - Enter a free IP in the private subnet This IP will not be used as the

management IP E.g., `192.168.200.200`
- **Security Group** – Select the NG Security Group created in Step 4.1



5. Click **Yes, Create**. The Network Interface is now listed in the Network Interface list

6. Select the Network Interface you just created and click **Attach.**
7. Select the Barracuda NG Firewall EC2 instance you created in step 5. E.g. **i-2adb8d65 Barracuda NG Firewall (running)**
8. Click **Yes, Attach**.



9. Right-click on the Network Interface you just created and select **Change Source/Dest. Check**.
10. Click **Yes, Disable**.
11. Go to the Amazon Web Services EC2 console (https://console.aws.amazon.com/ec2/home).
12. Right-click on the Barracuda NG Firewall Instance and click **Reboot**. You must reboot the Barracuda NG Firewall after adding additional Network Interfaces to make sure that the NG Firewall will detect and assign the correct network interface number to the new Elastic Network Interface.

Step 8. Create Route Tables

Create two routing tables to route the networks:

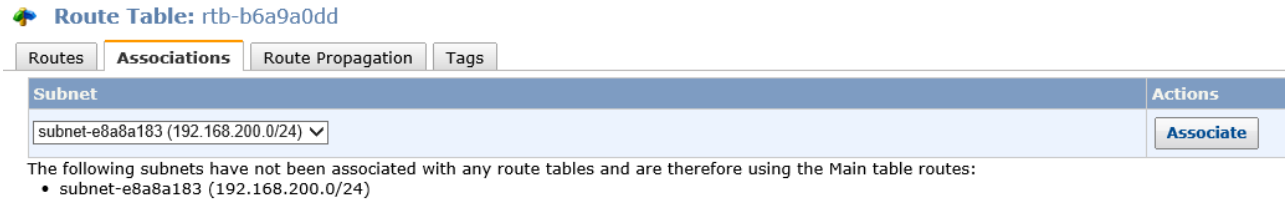
- A table to route traffic in the private network to the internal interface on the Barracuda NG Firewall.
- A table to route traffic from the Barracuda NG Firewall's external interface to the Internet gateway.

These route tables ensure that all traffic in the VPC passes through the Barracuda NG Firewall.

Step 8.1. Create a Route Table for the Private Network

Route all traffic in the private network to the eth1 interface on the Barracuda NG Firewall.

1. Go to the Amazon Web Services VPC console (https://console.aws.amazon.com/vpc/home).
2. In the left pane, click **Route Tables**.
3. Click **Create Route Table**.
4. Select the **VPC** with the 192.168.0.0./16 subnet (e.g., **vpc-abcd1234568 (192.168.0.0/16)**), and then click **Yes, Create**.
5. From the list of route tables on the page, select the route table that you just created.
6. In the lower pane, click the **Routes** tab and then add a routing entry with the following settings:
   - **Destination** – Enter `0.0.0.0/0`.
   - **Target** – Select **Enter network interface ID**, and then select the network interface in the private subnet you created in Step 7 (e.g., **eni-f39b8d87**). To find the network interface ID, go to the AWS EC2 console and click **Network Interfaces**. The network interface is in the 192.168.200.0/24 subnet.
7. Click **Add**.
8. Click the **Associations** tab.
9. From the **Select a subnet** list, select the 192.168.200.0/24 subnet (e.g., **subnet-d79be8bf (192.168.200.0/24)**).



10. Click **Associate**.
11. Click **Yes, Associate** to confirm the association.

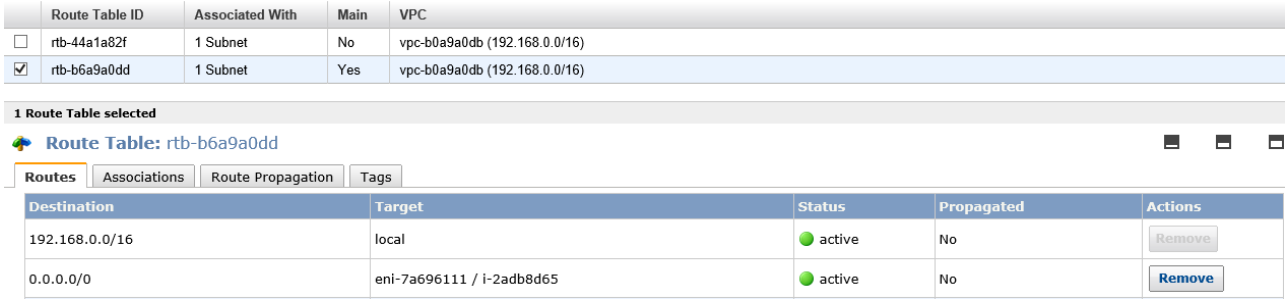
Step 8.2. Create a Route Table for the Public Network

Route traffic from the Barracuda NG Firewall's external interface to the Internet gateway that you created in Step 2.

1. Go to the Amazon Web Services VPC console (https://console.aws.amazon.com/vpc/home).
2. In the left pane, click **Route Tables**.
3. Click **Create Route Table**.
4. Select the **VPC** with the 192.168.0.0./16 subnet (e.g., **vpc-abcd1234568 (192.168.0.0/16)**), and then click **Yes, Create**.
5. From the list of route tables on the page, select the route table that you just created.
6. In the lower pane, click the **Routes** tab and then add a routing entry with the following settings:
   - **Destination** – Enter `0.0.0.0/0.`
   - **Target** – Select the Internet gateway that you created in Step 2 (e.g., **igw-6e81f206**).
7. Click **Add**.
8. Click the **Associations** tab.

9. From the **Select a subnet** list, select the 192.168.*XX*.0/24 subnet that you created in Step 3.2 (e.g., **subnet-2429574c (192.168.10.0./24)**).

10. Click **Associate**.
11. Click **Yes, Associate** to confirm the association.



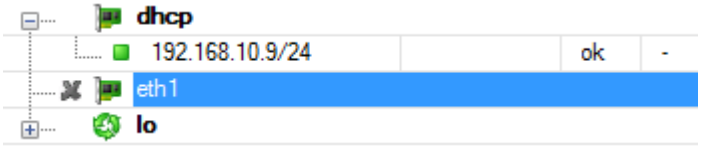
Your Barracuda NG Firewall instance is now reachable from the Internet.

Step 9. Add Amazon Network Interface to the Barracuda NG Firewall Instance

Add the second Amazon Network interface to the Barracuda NG Firewall Instance.

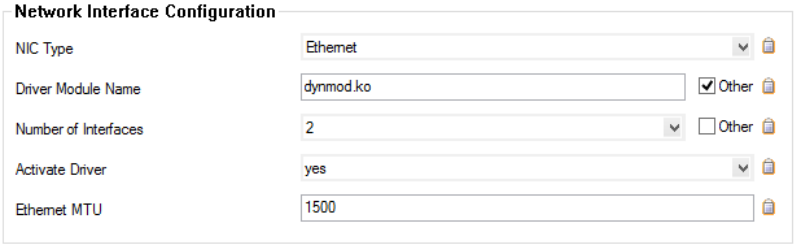
1. Reboot the Barracuda NG Firewall Instance, to correctly detect the new Network Interface.
2. With Barracuda NG Admin, log into the Barracuda NG Firewall. Use the following settings:
   - **Management IP**: The Amazon Elastic IP address that you created in Step 6 (e.g., `54.229.198.60`).
   - **Login**: `root`
   - **Password**: `<your Instance ID>` (e.g., `i-2adb8d65`)

     You have three days initial grace period to license your Barracuda NG Firewall, after that the default password (`ngf1r3wall`) also authenticates the root user.
3. Open the **Network** page (**CONTROL > Network).**
4. Ensure that there are two network interfaces listed: **dhcp** and **eth1**. if the second network interface is listed as eth0, reboot the Barracuda NG Firewall.

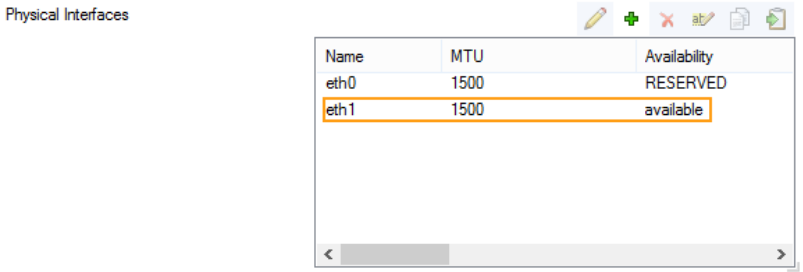


5. Open the **Network** configuration page (**CONFIG > Network**).
6. In the left pane click on **Interfaces.**
7. Click **Lock**.

8. Double Click on **10dynmod** entry in the **Network Interface Cards** list. The **Network Interface Cards: 10dynmod** window will open.
9. Select **2** from the **Number of Interfaces** drop down menu.
10. Click **OK**.



11. Click **Send Changes.** The eth1 interface is now listed in the **Physical Interface** list.



12. In the left pane click on **Routing**.
13. Click on **+** in the **Main Routing Table** section. The **Routes** windows opens.
14. Enter a **Name** for the route. E.g., `privateVPCSubnet`.
15. Configure the route with the following settings:
    - **Target Network Address** – Enter the destination address for the private subnet: `192.168.200.0/24`
    - **Route Type** – Select **directly attached network** from the drop down.
    - **Interface Name** – Select **eth1**.
    - **Trust Level** – Select **Trusted**.
16. Click **OK**.
17. Click **Send Changes**.
18. Click **Activate**.
19. Open the **Box** page (**CONTROL > Box**).
20. In the left pane in the **Network** section click **Activate new network configuration**. The **Network Activation** window opens.
21. Click on **Failsafe.**
22. Open **Server Properties** page for the **S1** virtual server (**CONFIG > Full Config > Virtual Servers > S1 > Server Properties**).
23. Click **Lock**.
24. Enter the IP address you assigned to the Amazon Network Interface in Step 8. in **Second-IP [IP2]**. E.g., `192.168.200.200`

    Do not change the **First IP** for the virtual server S1. You will lock yourself out if you do.
25. Select **yes** from the **Reply to Ping** drop down.
26. Click **Send Changes**.
27. Click **Activate**.

Additional Information

- Do not delete the default virtual server S1. By deleting the virtual server, the application redirect rule that lets you connect to the Barracuda NG Firewall EC2 is removed.
- When you add additional IP addresses to network interfaces or virtual servers on the Barracuda NG Firewall, you must also add these IP addresses to the respective Amazon network interfaces as additional IP addresses. Depending on the Amazon EC2 instance type used, there are limitations on the number of IP addresses that you can assign to a single Amazon network interface.
- To patch or update the Barracuda NG Firewall EC2 instance firmware, it is recommended that you use the Barracuda NG Admin graphic interface and not the SSH shell.

Troubleshooting Tips

- If you cannot activate the network after attaching an additional Amazon Network Interface make verify that the network interface numbering is correct. E.g., eth1 not eth0 if a dhcp device is already present. Reboot the Barracuda NG Firewall instance for the interface numbers to be assigned correctly.
- If you cannot connect to the other Amazon EC2 instances in the private subnet, check the following settings:
  - **Network Interfaces** – Mismatch between the IP address assigned to the network interface on the Barracuda NG Firewall and the Amazon Network Interface associated with it.
  - **Security Groups** – If the settings for the Security Group are too restrictive, the traffic will be blocked by the Amazon firewall. For debugging purposes, introduce a Security Group policy allowing all traffic in and out, and all traffic between the two security groups.
  - **Network ACLs** – If the rules in the Amazon network ACLs are too restrictive, traffic going into the subnet will be blocked by the Amazon firewall.
  - **Routing Tables** – Verify that the Amazon network interface associated with eth1 on the Barracuda NG Firewall is the default gateway for the private subnet and that the private subnet is associated with the correct routing table.
- If you cannot connect to the Internet from the Barracuda NG firewall, check the following settings:
  - **Security Groups** – If the settings for the Security Group are too restrictive, the traffic will be blocked by the Amazon firewall. For debugging purposes, introduce a Security Group policy allowing all traffic in and out, and all traffic between the two security groups.
  - **Network ACLs** – If the rules in the Amazon Network ACLs are too restrictive, traffic going into the subnet will be blocked by the Amazon firewall.
  - **Routing Tables** – Verify that the Amazon Internet Gateway (igw) is the default route and that the public subnet is associated with the correct routing table.

Next Steps

To continue setting up the Barracuda NG Firewall, you can proceed with the following tasks:

Task	Instructions
License the Barracuda NG Firewall. After the deployment you have an initial grace period of three days to license your Barracuda NG Firewall. After that the root user will also be able to log in with the default (ngf1r3wall) password.	How to Activate and License a Standalone Virtual Barracuda NG Firewall
Complete the Getting Started guide for the Barracuda NG Firewall.	Getting Started

Figures

1. AmazonCloudNG.png
2. AwsCreateVPC.png
3. AwsListVPCs.png
4. AwsCreateInternetGateway.png
5. AwsInternetGateway.png
6. AwsAssociateInternetGateway.png
7. AwsInternetGatewayFinished.png
8. AwsSubnetsList.png
9. Amazon_aws.png
10. AwsCreateNGSecurityGroup.png
11. AwsDefaultSecurityGroupList.png
12. AwsNetworkACL.png
13. EC2SearchMarketplace.png
14. awsLWchooseInstance.png
15. AWSwizardConfigureNetwork.png
16. AWSwizardConfigureStorage.png
17. awsLWConfSecurityGroup.png
18. awsLWkeyPair.png
19. awsLWDstSrcCheck.png
20. AwsEC2InstanceList.png
21. AwsAssociateElasticIP.png
22. AwsElasticIPList.png
23. AWSCreateNetworkInterface01.png
24. AWSCreateNetworkInterface02.png
25. AWSCreateNetworkInterface03.png
26. AwsRoutingPrivateNetworkAssociation.png
27. AwsRoutingPrivateNetwork.png
28. AwsRoutingPublicNetworkAssociation.png
29. AwsRoutingPrivateNetwork.png
30. AWSAddNItoNG01.png
31. AWSAddNItoNG02.png
32. AWSAddNItoNG03.png