AT&T

AMI Installation Guide, 17.2.0

November 2017

Supporting AT&T Vyatta Network Operating System

Contents

© 2017 AT&T Intellectual Property. All rights reserved. AT&T and Globe logo are registered trademarks of AT&T Intellectual Property.

© 2017 AT&T Intellectual Property. All rights reserved. AT&T and Globe logo are registered trademarks of AT&T Intellectual Property.

Copyright Statement

© 2017 AT&T Intellectual Property. All rights reserved. AT&T and Globe logo are registered trademarks of AT&T Intellectual Property. All other marks are the property of their respective owners.

The training materials and other content provided herein for assistance in training on the Vyatta vRouter may have references to Brocade as the Vyatta vRouter was formerly a Brocade product prior to AT&T's acquisition of Vyatta. Brocade remains a separate company and is not affiliated to AT&T.

About This Guide

This guide describes how to install AT&T Vyatta vRouter Amazon Machine Image (AMI) within the Amazon Web Services (AWS) cloud. The AT&T Vyatta vRouter is referred to as a virtual router, vRouter, or router in the guide.

© 2017 AT&T Intellectual Property. All rights reserved. AT&T and Globe logo are registered trademarks of AT&T Intellectual Property.

Installing the System

This chapter describes the AT&T Vyatta Amazon Machine Image (AMI) and how to install it within the Amazon Web Services (AWS) cloud.

Introduction

AWS is the cloud computing service from Amazon. It provides the tools and infrastructure that are required by businesses to run computing environments “within the cloud.”

When you operate a computing environment within the cloud, you reduce capital expenditures to a minimum and gain the ability to easily scale up or down your computing resources as required. You pay as you go and you pay only for the resources you use.

AWS provides several products and services to enable businesses to build the environments they require. At the core of AWS is the AMI, which is a virtual machine image. You instantiate a copy of the image as virtual machine instances within the AWS cloud. A variety of AMIs are available from a number of vendors. The Vyatta AMI is a version that is packaged to run in the AWS cloud. You can obtain the Vyatta AMI from the Amazon AWS Marketplace.

The Amazon Elastic Compute Cloud (EC2) is the AWS infrastructure within which all AMIs are launched. EC2 allows you to easily obtain and scale computing capacity as required.

A virtual private cloud (VPC) allows you to provision a virtual private network within the AWS cloud. A VPC allows you to define a virtual network topology within which you can create subnets, select IP addresses, and configure routing tables and network gateways.

This guide explains how to obtain and launch the Vyatta AMI into a VPC within the AWS cloud and to configure AWS such that you can access the AT&T Vyatta vRouter remotely. It also provides examples of how to configure the AT&T Vyatta vRouter to act as a NAT gateway, a site-to-site IPsec VPN endpoint, a site-to-site OpenVPN endpoint, or a remote access IPsec VPN server.

Before you begin

To use this guide and deploy the AT&T Vyatta vRouter within the AWS environment, you must be conversant with AWS and VPCs. It is assumed that you are thoroughly familiar with at least the following AWS documentation:

- http://docs.amazonwebservices.com/AWSEC2/latest/UserGuide/
- http://docs.amazonwebservices.com/AmazonVPC/latest/UserGuide/

You must also be knowledgeable about the AWS services you are using. You can get AWS documentation at http://aws.amazon.com/documentation/.

The following requirements about AWS are also assumed.

AWS Account

- You have an AWS account. Sign up for an AWS account at http://aws.amazon.com/.
- You are able to log on to the AWS Management Console.

AWS Skills

- You have mastered general AWS skills, including the following:
    - Creating a VPC subnet
    - Creating and attaching an Amazon VPC Internet gateway to the VPC
    - Setting up routing in the VPC to enable traffic to flow between the VPC subnet and the Internet
    - Setting up a security group to control inbound and outbound traffic for the instances that are launched within the VPC
    - Launching an AMI instance (either Linux, UNIX, or Windows) into the VPC

© 2017 AT&T Intellectual Property. All rights reserved. AT&T and Globe logo are registered trademarks of AT&T Intellectual Property.

- Creating a key pair and assigning it to an instance
- Assigning an Elastic IP address to an instance
- Connecting to an instance remotely by using SSH (for Linux or UNIX instances) or RDP (for Windows instances)

Learning about AWS

The use of AWS is beyond the scope of this guide. Before trying to use a Vyatta AMI with AWS, review the AWS documentation listed in Table 1 *(page 7)*.

Table 1: Amazon web services reference documentation

Topic	Location
AWS	
Introduction to AWS webinar in the Solutions playlist	http://aws.amazon.com/resources/webinars
AWS documentation library	http://aws.amazon.com/documentation
Amazon EC2	
Amazon EC2 documentation index	http://aws.amazon.com/documentation/ec2
Amazon EC2 Getting Started Guide	http://docs.amazonwebservices.com/AWSEC2/latest/GettingStartedGuide
Amazon EC2 User Guide	http://docs.amazonwebservices.com/AWSEC2/latest/UserGuide
Amazon VPC documentation index	http://aws.amazon.com/documentation/vpc
Amazon VPC	
Amazon VPC Getting Started Guide	http://docs.amazonwebservices.com/AmazonVPC/latest/GettingStartedGuide
Amazon VPC User Guide	http://docs.amazonwebservices.com/AmazonVPC/latest/UserGuide

Installation options

This guide describes how to install a Vyatta AMI into a VPC within the AWS environment as this is how it is most likely to be deployed.

Creating a VPC

Before you obtain a Vyatta AMI, you must create a VPC into which the AMI can be launched. You can create a VPC with a single public subnet by following the steps outlined in Amazon VPC Getting Started Guide.

For the example that follows, it is assumed that you are logged on to the AWS Management Console and have completed the steps in Amazon VPC Getting Started Guide. Amazon VPC Getting Started Guide. These steps create a VPC that provides for addresses in the range of 10.0.0.0/16 and a public subnet in the range of

© 2017 AT&T Intellectual Property. All rights reserved. AT&T and Globe logo are registered trademarks of AT&T Intellectual Property.

10.0.0.0/24. The example uses these addresses, but any ranges of private IP addresses that are defined in RFC 1918 (that is, 10.0.0.0/8, 172.16.0.0/12, or 192.168.0.0/16) can be used.

Modifying the default security group

Security groups provide the policies that control traffic flow and access for EC2 instances and instances within a VPC. EC2 security groups and VPC security groups are independent of each another. EC2 security groups cannot be used for instances within a VPC, and VPC security groups cannot be used for EC2 instances (that is, instances not associated with a VPC). Vyatta AMI instances are launched into VPCs, so they use VPC security groups.

The default VPC security group allows instances within the VPC to communicate with one another and to access the Internet, but it does not allow remote access to the AMI instance or instances that you create within the VPC. To provide remote SSH access to the VPC, either create a new security group or modify the default security group. The following example shows how to modify the default security group to allow SSH access from anywhere.

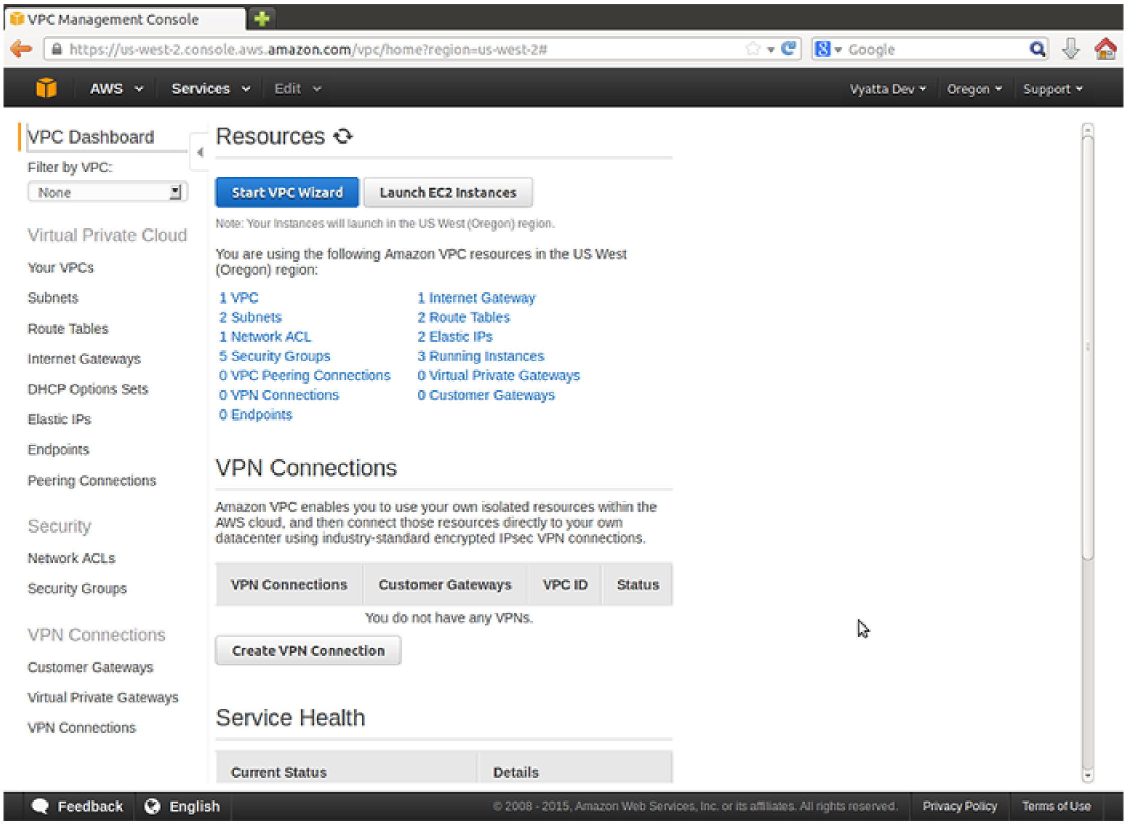
> **Note:** This example shows how to allow SSH access from anywhere for testing purposes only. In general, it is best to restrict SSH access to source addresses that you control. Change the port to something other than 22 or 2222. Also, make sure you change the default password on all devices in your network.

To modify the default security group to allow SSH access

1. On the **AWS Management Console Home** page, click **VPC**.

   Info:

   The **Amazon VPC Console Dashboard** page appears.



Note: Your instances will launch in the US West (Oregon) region.

You are using the following Amazon VPC resources in the US West (Oregon) region:

1 VPC	1 Internet Gateway
2 Subnets	2 Route Tables
1 Network ACL	2 Elastic IPs
5 Security Groups	3 Running Instances
0 VPC Peering Connections	0 Virtual Private Gateways
0 VPN Connections	0 Customer Gateways
0 Endpoints	

VPN Connections

Amazon VPC enables you to use your own isolated resources within the AWS cloud, and then connect those resources directly to your own datacenter using industry-standard encrypted IPsec VPN connections.

VPN Connections	Customer Gateways	VPC ID	Status

You do not have any VPNs.

Service Health

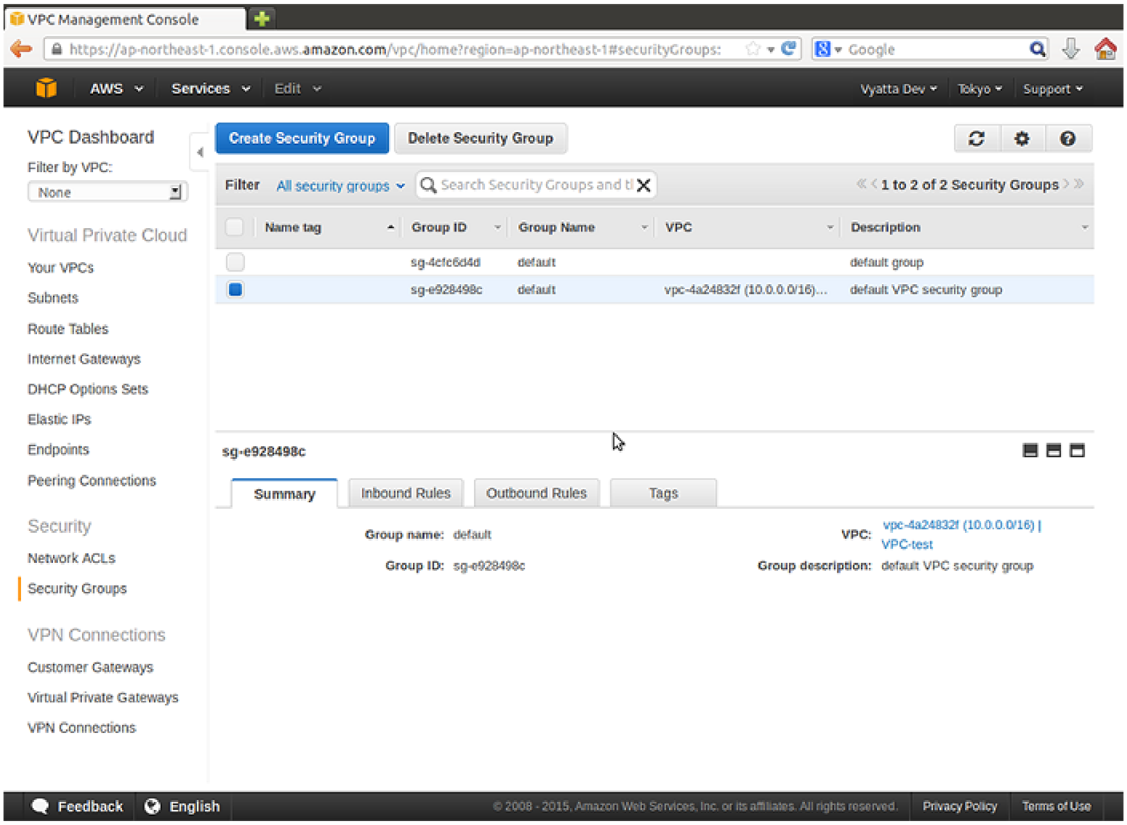
Current Status	Details

© 2008 - 2015, Amazon Web Services, Inc. or its affiliates. All rights reserved.

2. In the left navigation pane, select **Security Groups**. The **Security Groups** page opens on the right.
3. Select the **default** security group. The details for the **default** security group appear at the bottom of the page.

   Info:

© 2017 AT&T Intellectual Property. All rights reserved. AT&T and Globe logo are registered trademarks of AT&T Intellectual Property.



	Name tag	Group ID	Group Name	VPC	Description
□		sg-4cfc6d4d	default		default group
■		sg-e928498c	default	vpc-4a24832f (10.0.0.0/16)...	default VPC security group

sg-e928498c

Group name: default

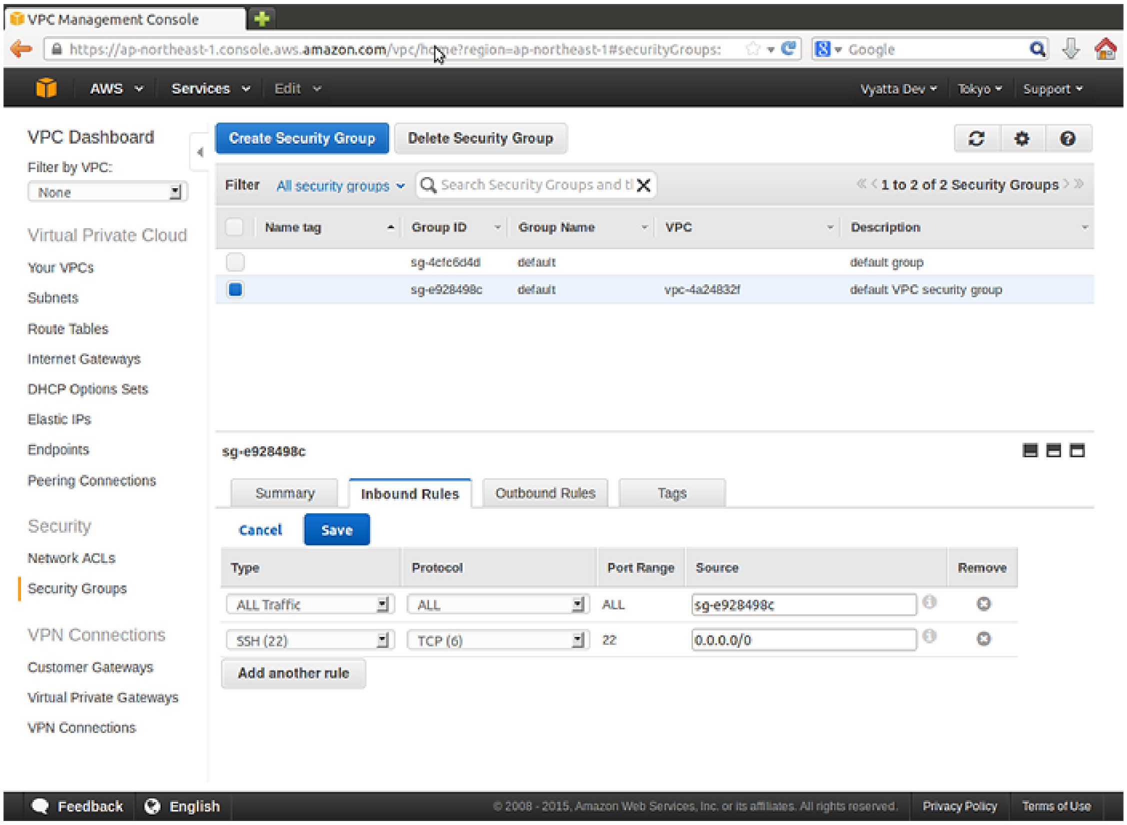
Group ID: sg-e928498c

VPC: vpc-4a24832f (10.0.0.0/16) | VPC-test

Group description: default VPC security group

4. Click the **Inbound Rules** tab. The default inbound rule appears. This rule provides access between the instances that use this security group.
5. Click **Edit** and then click **Add another rule** to add new rules. Select **SSH** from the drop#down menu.

Info:



Name tag	Group ID	Group Name	VPC	Description
	sg-4cfc6d4d	default		default group
	sg-e928498c	default	vpc-4a24832f	default VPC security group

sg-e928498c

Type	Protocol	Port Range	Source	Remove
ALL Traffic	ALL	ALL	sg-e928498c	⊗
SSH (22)	TCP (6)	22	0.0.0.0/0	⊗

6. In the **Source** field, enter 0.0.0.0/0 and click **Add another Rule**. The rule appears in the rule table to the right. Click **Save** to apply the rule change. The security group now allows SSH access from anywhere.

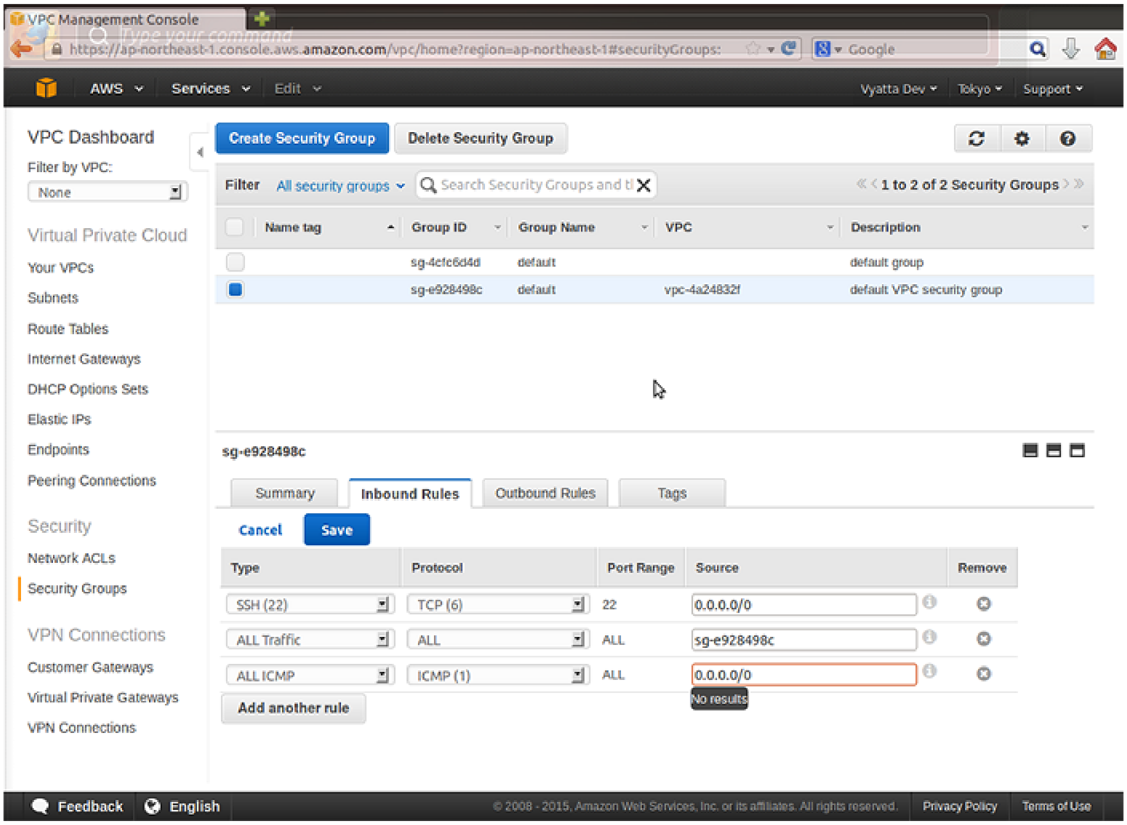
   Info:

   The default VPC security group does not allow instances within the VPC to respond to pings (ICMP echo requests) from remote devices. In many cases this is desirable. We want to determine that an instance is reachable for testing purposes, so we allow ICMP traffic. This example shows how to modify the default security group to allow incoming ICMP traffic from anywhere.

   To modify the default VPC security group to allow ICMP traffic

7. Click **Edit** and then click **Add another rule** to add new rules. Select **ALL ICMP** from the drop#down menu.

   Info:



Name tag	Group ID	Group Name	VPC	Description
	sg-4cfc6d4d	default		default group
	sg-e928498c	default	vpc-4a24832f	default VPC security group

Type	Protocol	Port Range	Source	Remove
SSH (22)	TCP (6)	22	0.0.0.0/0	
ALL Traffic	ALL	ALL	sg-e928498c	
ALL ICMP	ICMP (1)	ALL	0.0.0.0/0	

8. In the **Source** field, enter 0.0.0.0/0 and click **Save**. The rule appears in the rule table to the right. The security group now allows ICMP traffic from anywhere.

   Info:

Obtaining and launching the Vyatta AMI

This section presents the following topic:

- Obtaining the Vyatta AMI from the EC2 console *(page 11)*

The Vyatta AMI comes preconfigured as a standard AT&T Vyatta vRouter with some additional configuration changes to ease installation and access within AWS:

- The dp0s0 interface is configured to use DHCP. The IP address can be specified when launching the instance. If an IP address is not specified, AWS assigns one automatically. The IP address is in the range of private addresses for the subnet into which it is launched.
- SSH access is configured.

Note: The Vyatta AMI is supported as a M4.Large, M4.XLarge, M4.2XLarge, and M4.4XLarge instance within AWS and is provided with persistent Amazon Elastic Block Storage (EBS).

Note: The AT&T Vyatta vRouter supports HVM AMI only.

To obtain the AMI, refer to Obtaining the Vyatta AMI from the EC2 console *(page 11)*.

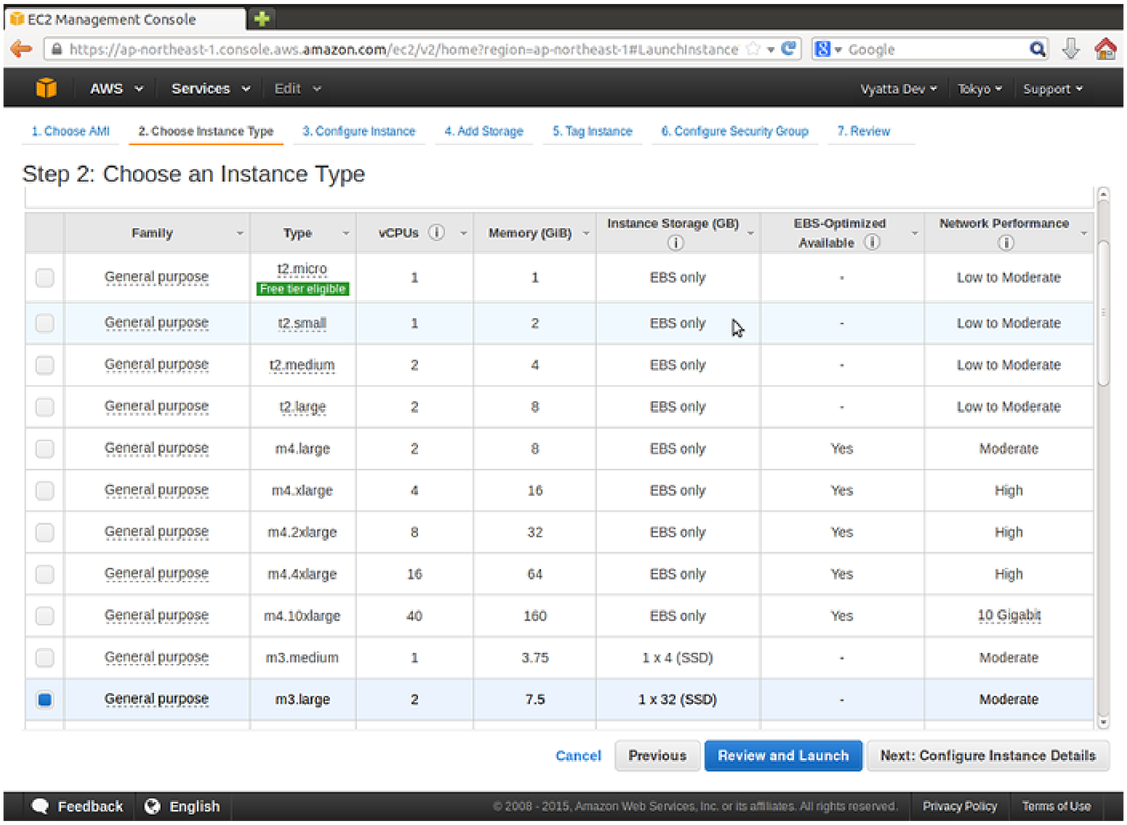
Obtaining the Vyatta AMI from the EC2 console

To obtain and launch the Vyatta AMI from the EC2 Console

© 2017 AT&T Intellectual Property. All rights reserved. AT&T and Globe logo are registered trademarks of AT&T Intellectual Property.

1. Click **EC2** on the **AWS Management Console Home** page. The **Amazon EC2 Console Dashboard** page appears.
2. Select **AMIs** in the left navigation pane. The **Amazon Machine Images** page opens on the right.
3. In the **Viewing** field, select **Private Images**, and specify vyatta-ami as the search string. Vyatta AMIs are listed.
4. Select a Vyatta AMI and click **Launch** at the top of the **Amazon Machine Images** page. The **Request Instances Wizard** opens at the **Instance Details** step.

   Info:

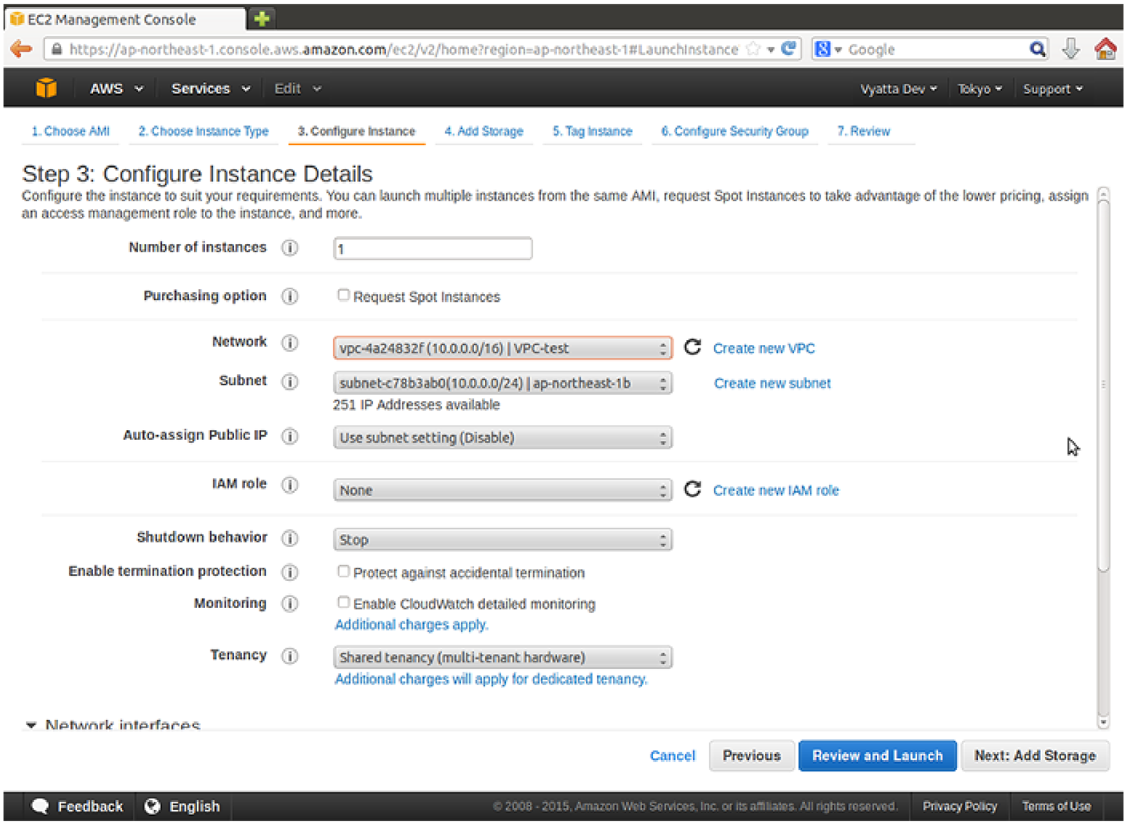

EC2 Management Console
https://ap-northeast-1.console.aws.amazon.com/ec2/v2/home?region=ap-northeast-1#LaunchInstance
Google
AWS
Services
Edit
Vyatta Dev
Tokyo
Support
1. Choose AMI
2. Choose Instance Type
3. Configure Instance
4. Add Storage
5. Tag Instance
6. Configure Security Group
7. Review
Cancel
Previous
Review and Launch
Next: Configure Instance Details
Feedback
English
© 2008 - 2015, Amazon Web Services, Inc. or its affiliates. All rights reserved.
Privacy Policy
Terms of Use

Step 2: Choose an Instance Type

	Family	Type	vCPUs	Memory (GiB)	Instance Storage (GB)	EBS-Optimized Available	Network Performance
□	General purpose	t2.micro Free tier eligible	1	1	EBS only	-	Low to Moderate
□	General purpose	t2.small	1	2	EBS only	-	Low to Moderate
□	General purpose	t2.medium	2	4	EBS only	-	Low to Moderate
□	General purpose	t2.large	2	8	EBS only	-	Low to Moderate
□	General purpose	m4.large	2	8	EBS only	Yes	Moderate
□	General purpose	m4.xlarge	4	16	EBS only	Yes	High
□	General purpose	m4.2xlarge	8	32	EBS only	Yes	High
□	General purpose	m4.4xlarge	16	64	EBS only	Yes	High
□	General purpose	m4.10xlarge	40	160	EBS only	Yes	10 Gigabit
□	General purpose	m3.medium	1	3.75	1 x 4 (SSD)	-	Moderate
■	General purpose	m3.large	2	7.5	1 x 32 (SSD)	-	Moderate

5. Choose a listed instance type (refer to the preceding figure) to launch the Vyatta AMI instance into a VPC. Then, in the **Network** area, select **VPC** and select the subnet in the VPC into which you want to launch the instance.

   Info:



Step 3: Configure Instance Details

Configure the instance to suit your requirements. You can launch multiple instances from the same AMI, request Spot Instances to take advantage of the lower pricing, assign an access management role to the instance, and more.

Number of instances: 1

Purchasing option: □ Request Spot Instances

Network: vpc-4a24832f (10.0.0.0/16) | VPC-test — Create new VPC

Subnet: subnet-c78b3ab0(10.0.0.0/24) | ap-northeast-1b — Create new subnet
251 IP Addresses available

Auto-assign Public IP: Use subnet setting (Disable)

IAM role: None — Create new IAM role

Shutdown behavior: Stop

Enable termination protection: □ Protect against accidental termination

Monitoring: □ Enable CloudWatch detailed monitoring
Additional charges apply.

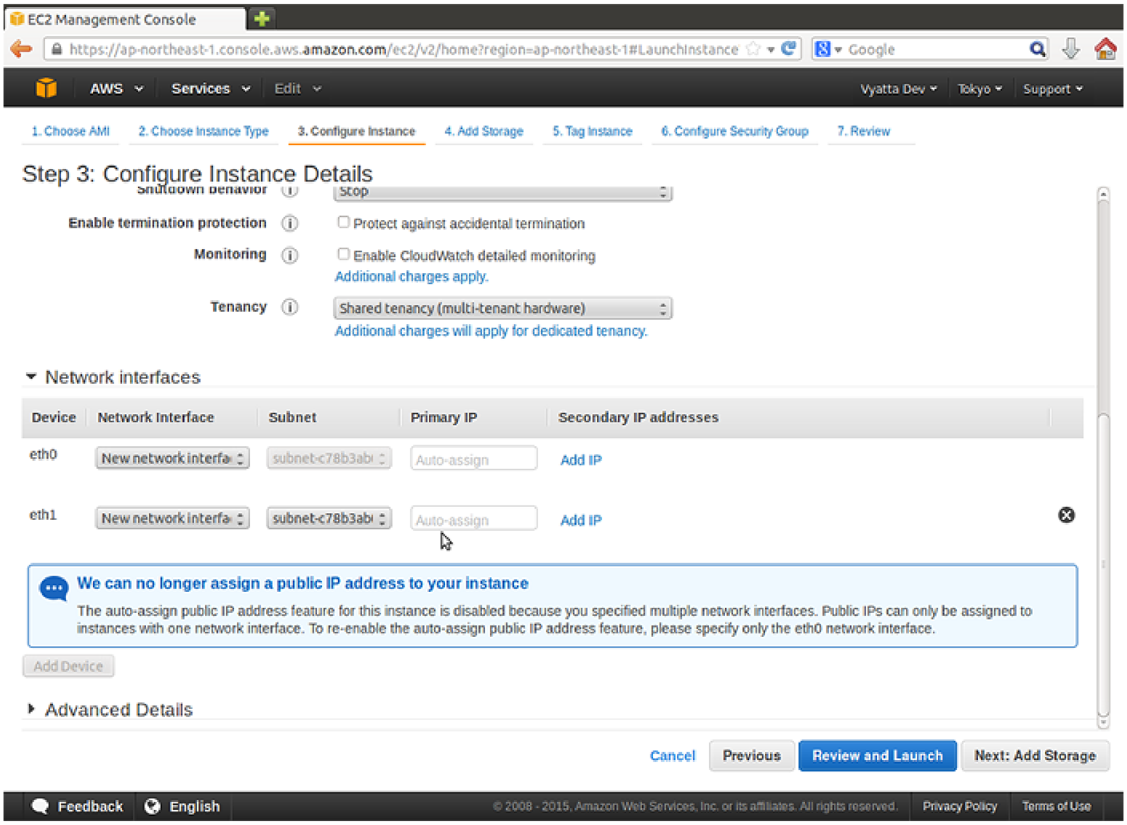
Tenancy: Shared tenancy (multi-tenant hardware)
Additional charges will apply for dedicated tenancy.

▾ Network interfaces

6. If you want to use a static IP address, specify the address in the **IP Address** field. If you want to include more than one network interface, you can add the second network interface and configure it as required. Click **Add Storage** to configure additional instance details.

   Info:

   Note: Vyatta AMI supports two interfaces for each instance.



Step 3: Configure Instance Details

Shutdown behavior: Stop

Enable termination protection: □ Protect against accidental termination

Monitoring: □ Enable CloudWatch detailed monitoring
Additional charges apply.

Tenancy: Shared tenancy (multi-tenant hardware)
Additional charges will apply for dedicated tenancy.

Network interfaces

Device	Network Interface	Subnet	Primary IP	Secondary IP addresses
eth0	New network interfa	subnet-c78b3ab	Auto-assign	Add IP
eth1	New network interfa	subnet-c78b3ab	Auto-assign	Add IP

We can no longer assign a public IP address to your instance

The auto-assign public IP address feature for this instance is disabled because you specified multiple network interfaces. Public IPs can only be assigned to instances with one network interface. To re-enable the auto-assign public IP address feature, please specify only the eth0 network interface.

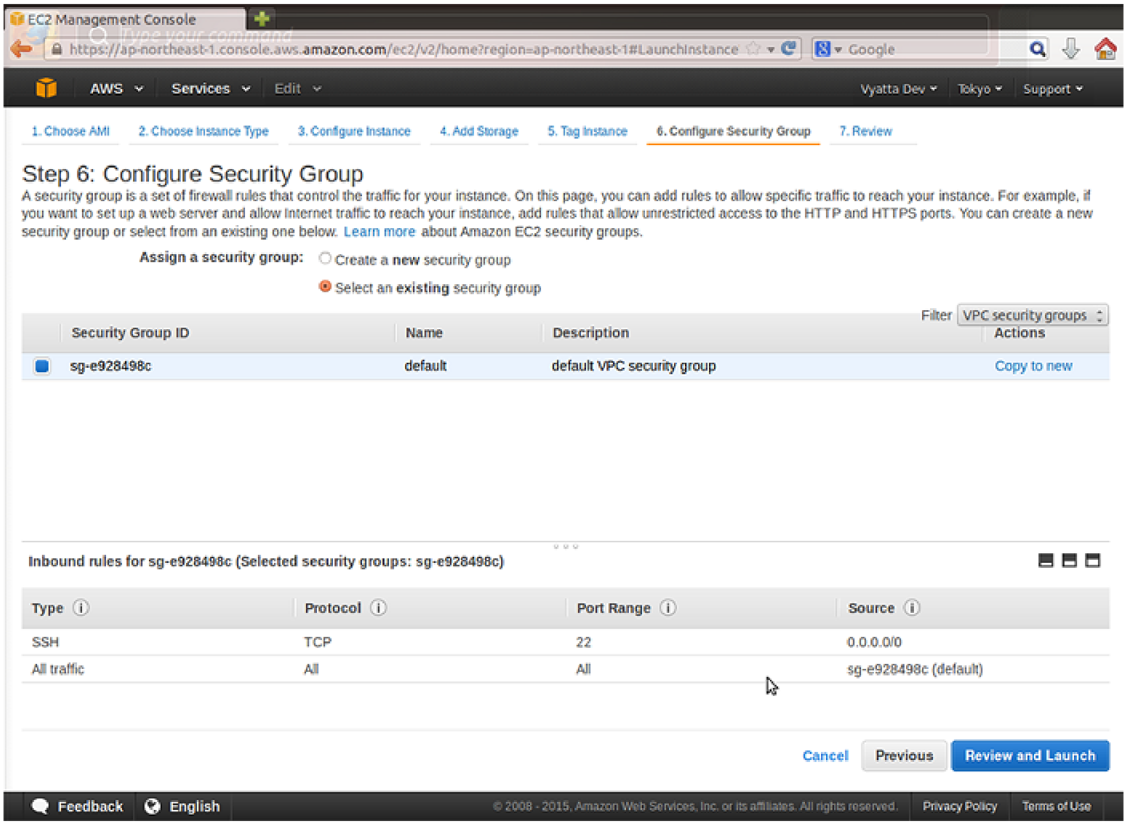
Advanced Details

© 2008 - 2015, Amazon Web Services, Inc. or its affiliates. All rights reserved.

You can modify the storage configuration, if required.

7. Click **Tag Instance** to continue.
8. To add tags (for example, a name) to your instance, specify a key and an associated value. In this case, we have chosen a name of R1.
9. Click **Configure Security Group** to continue.
10. Configure a security group by creating a new group or selecting an existing one.

Info:



Step 6: Configure Security Group

A security group is a set of firewall rules that control the traffic for your instance. On this page, you can add rules to allow specific traffic to reach your instance. For example, if you want to set up a web server and allow Internet traffic to reach your instance, add rules that allow unrestricted access to the HTTP and HTTPS ports. You can create a new security group or select from an existing one below. Learn more about Amazon EC2 security groups.

Assign a security group: ○ Create a **new** security group

● Select an **existing** security group

Filter: VPC security groups

	Security Group ID	Name	Description	Actions
■	sg-e928498c	default	default VPC security group	Copy to new

Inbound rules for sg-e928498c (Selected security groups: sg-e928498c)

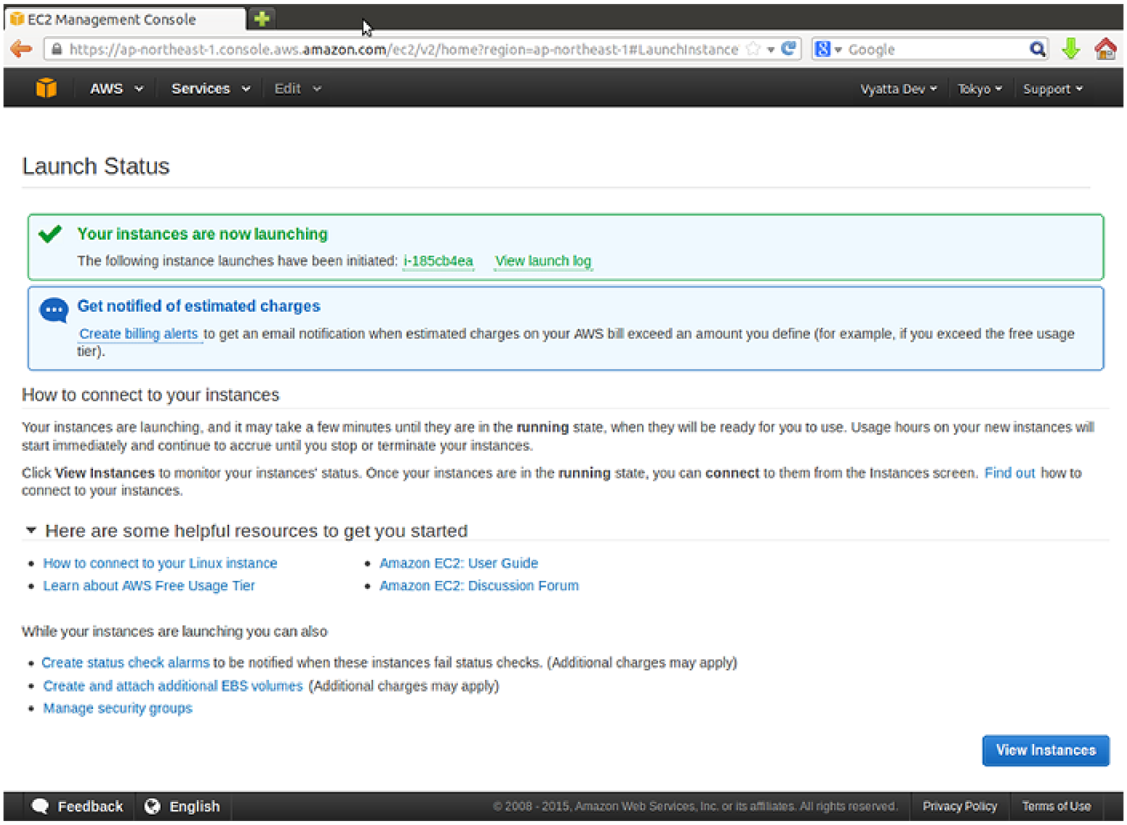
Type	Protocol	Port Range	Source
SSH	TCP	22	0.0.0.0/0
All traffic	All	All	sg-e928498c (default)

11. Click **Launch** to continue.
12. You must select **Create a new Key Pair** (or **Choose from your existing Key Pairs** if you have already created them) because the AT&T Vyatta vRouter requires public/private key pairs for authentication within AWS. Enter a name for the key pair in the **Enter a name for your key pair** field (in this case we entered **R1key**). Click the **Download your Key Pair**. Save the .pem key pair file; SSH uses it to access the Vyatta AMI remotely in a later step. You will move to the **Launch Instance** page.

    Info:

    The **Launch Instance Wizard** page appears.

© 2017 AT&T Intellectual Property. All rights reserved. AT&T and Globe logo are registered trademarks of AT&T Intellectual Property.


EC2 Management Console
https://ap-northeast-1.console.aws.amazon.com/ec2/v2/home?region=ap-northeast-1#LaunchInstance
Google
AWS
Services
Edit
Vyatta Dev
Tokyo
Support

Launch Status

Your instances are now launching

The following instance launches have been initiated: i-185cb4ea View launch log

Get notified of estimated charges

Create billing alerts to get an email notification when estimated charges on your AWS bill exceed an amount you define (for example, if you exceed the free usage tier).

How to connect to your instances

Your instances are launching, and it may take a few minutes until they are in the **running** state, when they will be ready for you to use. Usage hours on your new instances will start immediately and continue to accrue until you stop or terminate your instances.

Click **View Instances** to monitor your instances' status. Once your instances are in the **running** state, you can **connect** to them from the Instances screen. Find out how to connect to your instances.

Here are some helpful resources to get you started

- How to connect to your Linux instance
- Learn about AWS Free Usage Tier
- Amazon EC2: User Guide
- Amazon EC2: Discussion Forum

While your instances are launching you can also

- Create status check alarms to be notified when these instances fail status checks. (Additional charges may apply)
- Create and attach additional EBS volumes (Additional charges may apply)
- Manage security groups

View Instances
Feedback
English
© 2008 - 2015, Amazon Web Services, Inc. or its affiliates. All rights reserved.
Privacy Policy
Terms of Use

13. Click **View Instances** to return to the Amazon EC2 Console.

    Info:

    At this point, the Vyatta AMI instance is running within your VPC. The next step is to assign an Elastic IP address to the Vyatta AMI instance. Refer to Assigning an AWS elastic IP address to the instance *(page 16)*.

Assigning an AWS elastic IP address to the instance

To access the instance remotely, you assign an AWS Elastic IP address to it.

To assign an Elastic IP address

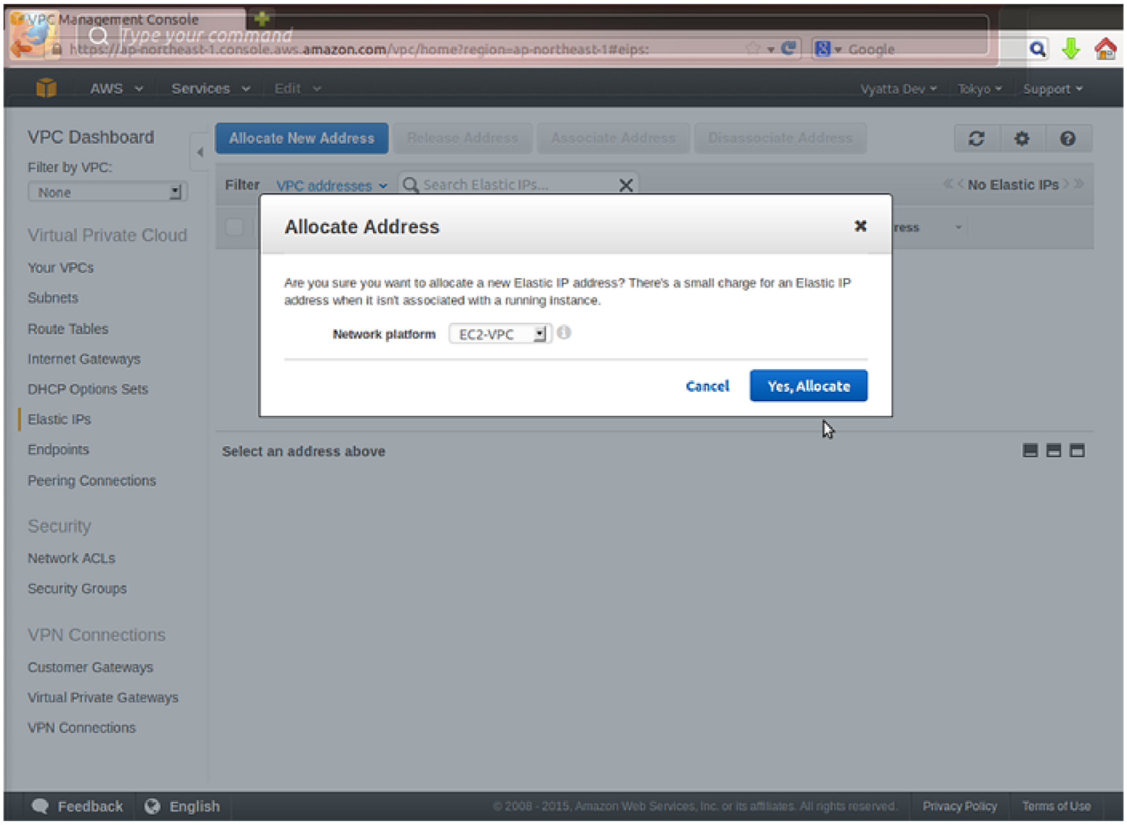
1. Click **VPC** on the **AWS Management Console Home** page. The **Amazon VPC Console Dashboard** page appears.
2. In the left navigation pane, select **Elastic IPs**. The **Addresses** pane opens.

    Info:

3. If an Elastic IP address is not already available to you, click **Allocate New Address**. The **Allocate Address** dialog box opens.

    Info:

© 2017 AT&T Intellectual Property. All rights reserved. AT&T and Globe logo are registered trademarks of AT&T Intellectual Property.



Allocate Address

Are you sure you want to allocate a new Elastic IP address? There's a small charge for an Elastic IP address when it isn't associated with a running instance.

Network platform: EC2-VPC

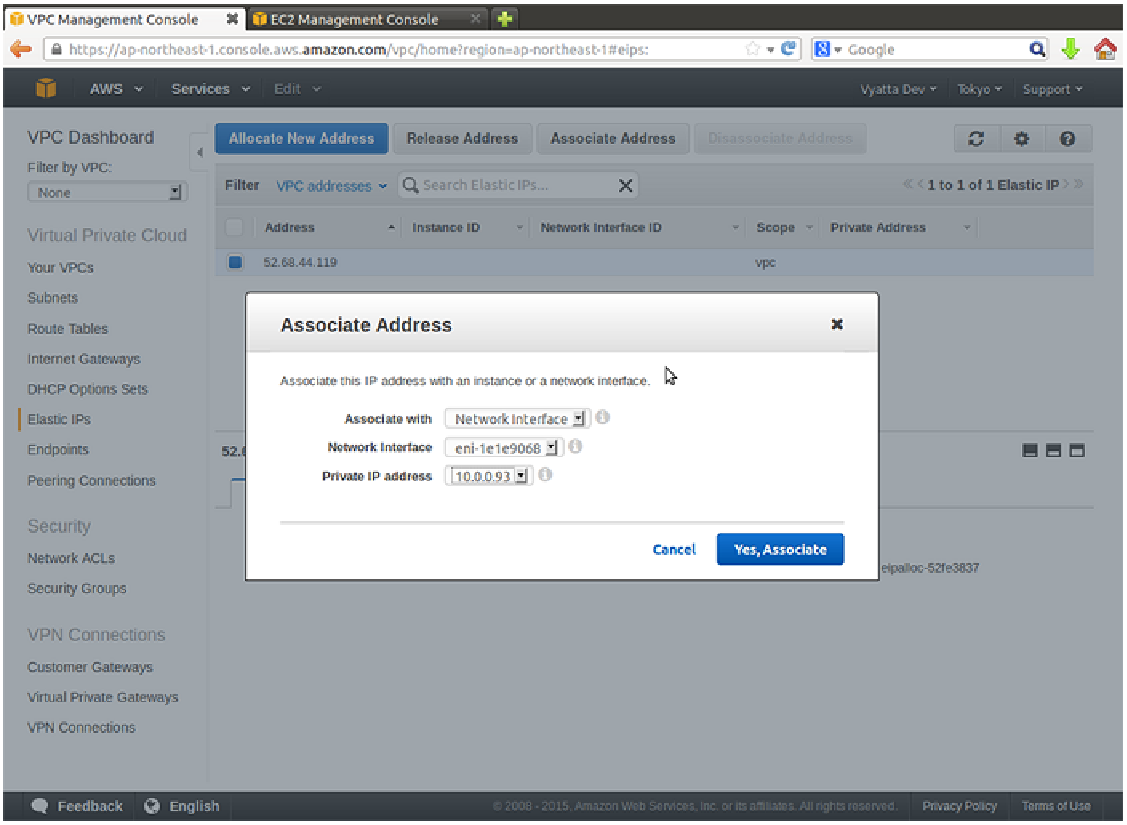
4. In the **Network platform** field, select **EC2#VPC**. Click **Yes, Allocate**. A new Elastic IP address appears on the **Addresses** page.

   Info:

5. Select the Elastic IP address to be associated with the instance you launched. Click **Associate Address**. The **Associate Address** dialog box opens.

   Info:

© 2017 AT&T Intellectual Property. All rights reserved. AT&T and Globe logo are registered trademarks of AT&T Intellectual Property.



Associate Address

Associate this IP address with an instance or a network interface.

Associate with: Network Interface

Network Interface: eni-1e1e9068

Private IP address: 10.0.0.93

6. In the **Associate with** field, select the network interface for eth0. Click **Yes, Associate**. The Elastic IP address is associated with the instance that you created. This association appears on the **Addresses** pane.

   Info:

Accessing the instance remotely

After you have modified the security group that is associated with the instance to allow access from SSH and you have provided the instance with an Elastic IP address, you can test your access to it.

1. On a remote machine, open an SSH session. As the destination address, provide the Elastic IP address that you associated with the instance. You also have to provide the location of the key file that you created during the Vyatta AMI configuration in a previous step. Refer to the documentation for the SSH client that you are using for details on how to specify these parameters.

   Info:

   > **Note:** On Linux and UNIX systems, use the `ssh` command. On Windows machines, use a program such as putty for SSH access. In both cases, the .pem file must be converted to a key file that has a .ppk format with a tool such as ssh-keygen or puttygen. This key file is then used by SSH or putty to access the instance remotely.

2. After you are connected, you see the login as: prompt. Log on as the vyatta user.

Terminating an instance

If you terminate a Vyatta instance, make sure you also remove the storage volume that is attached to the instance (unless you want to reuse it). Unless you explicitly delete the storage volume, you are charged for it.

© 2017 AT&T Intellectual Property. All rights reserved. AT&T and Globe logo are registered trademarks of AT&T Intellectual Property.

Note: To start, stop, or reboot an instance, use the AWS GUI and not the vRouter CLI.

© 2017 AT&T Intellectual Property. All rights reserved. AT&T and Globe logo are registered trademarks of AT&T Intellectual Property.

Configuration Examples

This chapter presents examples of configuring an AT&T Vyatta Amazon Machine Image (AMI) instance for various scenarios.

Creating a NAT device

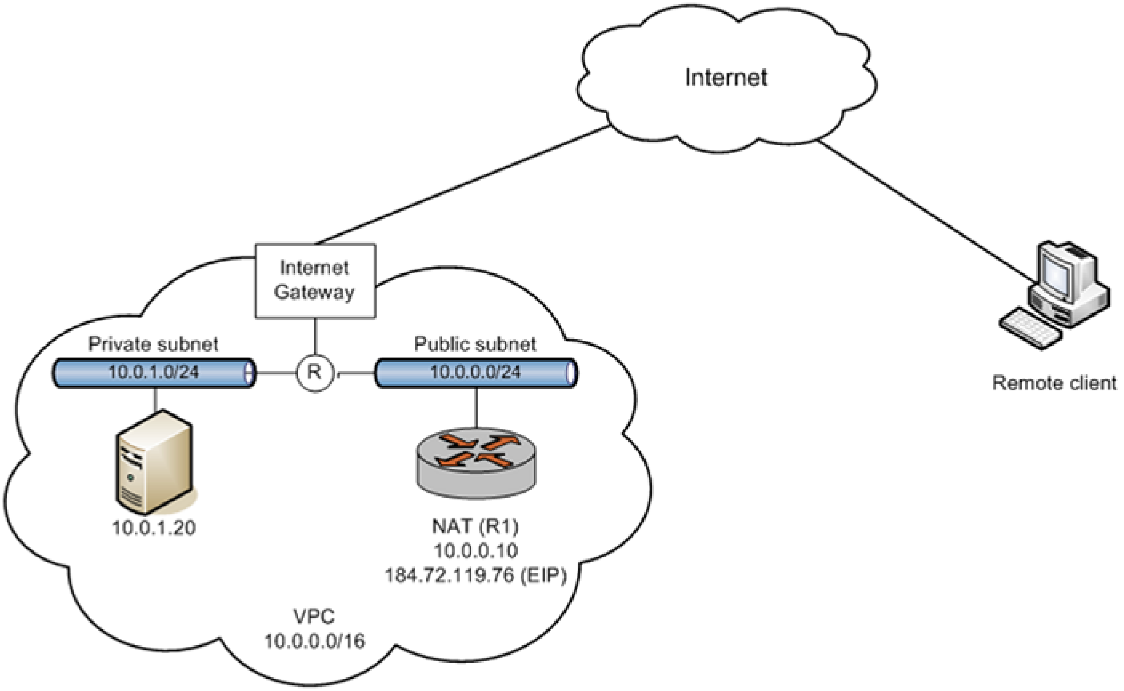
At the end of the installation procedure in the preceding section, the following prerequisites for the examples in this chapter were completed:

- A Vyatta AMI instance was launched into an existing Virtual Private Cloud (VPC) with a single public subnet.
- The default security group was modified to allow SSH access and ICMP traffic.
- An Elastic IP address was assigned to the interface of the instance.
- Remote SSH access was tested.

In this example, the following steps are completed:

- The Vyatta AMI instance is configured as a Network Address Translation (NAT) device.
- A new subnet is created within the VPC.
- A routing table is configured so that the subnet can route traffic through the Vyatta NAT device.
- A new instance is launched within the new subnet.
- Remote access to the instance in the new subnet is tested by using SSH.

The following diagram shows the configuration that is created.



Configure the Vyatta AMI instance for NAT

To configure the Vyatta AMI instance to act as a NAT device

1. Log on to the Vyatta AMI instance by using the SSH client. Refer to "Accessing the Instance Remotely" on page 17 *(page 20)*.
2. Enter configuration mode.

© 2017 AT&T Intellectual Property. All rights reserved. AT&T and Globe logo are registered trademarks of AT&T Intellectual Property.

Info:

```
vyatta@vyatta:~$ configure

[edit]
```

3. Change the host name to R1 to identify the instance.

   Info:

```
vyatta@vyatta# set system host-name R1

[edit]
```

   The command prompt changes to reflect the new host name the next time you log on.

4. Configure masquerade NAT for outbound traffic from subnet 10.0.1.0/24. (This network address represents the private subnet to be created in a later step.)

   Info:

```
vyatta@vyatta# set service nat source rule 10
[edit]
vyatta@vyatta# set service nat source rule 10 outbound-interface dp0s0
[edit]
vyatta@vyatta# set service nat source rule 10 translation address masquerade
[edit]
vyatta@vyatta# set service nat source rule 10 source address 10.0.1.0/24
[edit]
```

5. Configure the destination NAT to provide remote access to an instance in the private subnet. The NAT rule passes connections to port 3333 to address 10.0.1.20 port 22. (This instance is launched in a later step.)

   Info:

```
vyatta@vyatta# set service nat destination rule 20 destination port 3333
[edit]
vyatta@vyatta# set service nat destination rule 20 protocol tcp
[edit]
vyatta@vyatta# set service nat destination rule 20 translation address 10.0.1.20
[edit]
vyatta@vyatta# set service nat destination rule 20 inbound-interface dp0s0
[edit]
vyatta@vyatta# set service nat destination rule 20 translation port 22
[edit]
```

6. Commit and save the changes.

   Info:

```
vyatta@vyatta# commit
[edit]
vyatta@vyatta# save
Saving configuration to '/config/config.boot'...
Done
[edit]
```

7. View the NAT#related changes.

   Info:

```
vyatta@vyatta# show service
 service {
        nat {
                destination {
                        rule 20 {
                                destination {
                                        port 3333
```

© 2017 AT&T Intellectual Property. All rights reserved. AT&T and Globe logo are registered trademarks of AT&T Intellectual Property.

```
                                }
                                inbound-interface dp0s0
                                protocol tcp
                                translation {
                                        address 10.0.1.20
                                        port 22
                                }
                        }
                }
                source {
                        rule 10 {
                                outbound-interface dp0s0
                                source {
                                        address 10.0.1.0/24
                                }
                                translation {
                                        address masquerade
                                }
                        }
                }
        }
        ssh
 }
[edit]
```

8. Exit configuration mode and then exit the logon session.

   Info:

   ```
   vyatta@vyatta# exit
   exit
   vyatta@vyatta:~$ exit

   logout
   ```

   The SSH session is terminated.

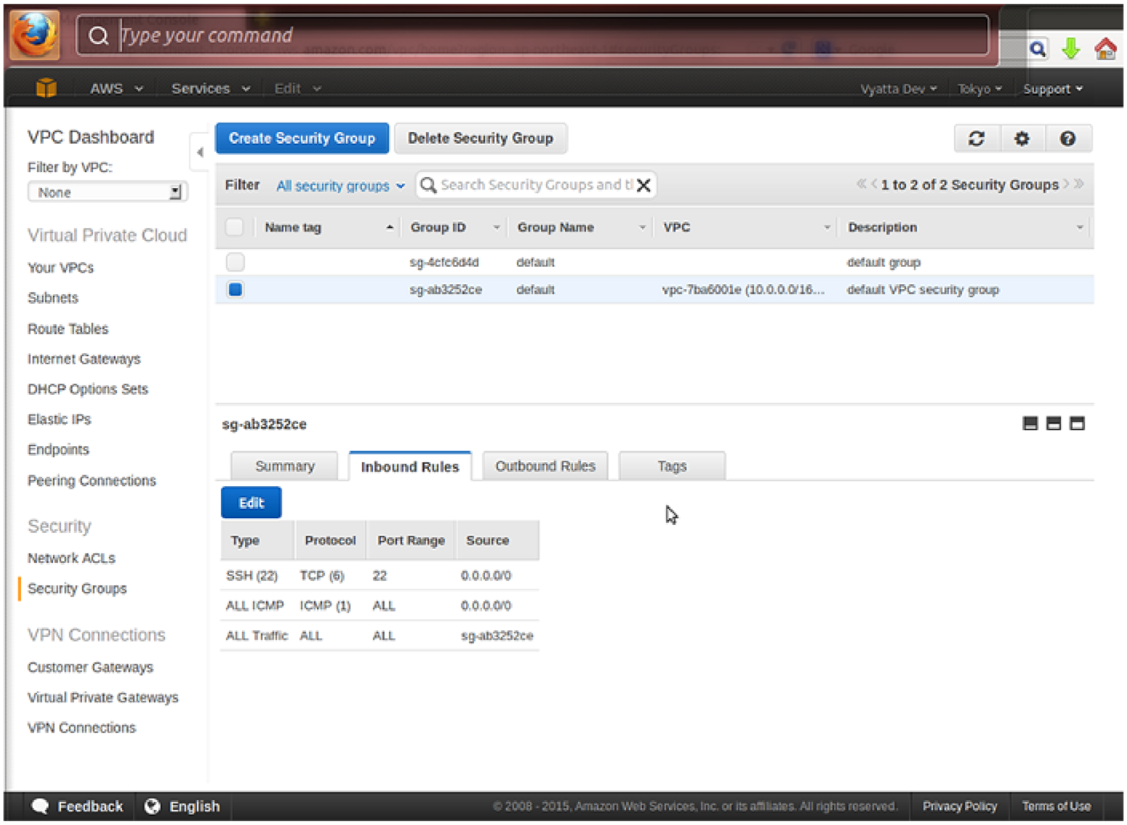
Modify the default security group

This example shows how to modify the default security group to allow port 3333 access from anywhere. Connections to the Elastic IP address on port 3333 are translated by the Vyatta NAT device and then routed to the private instance that is created in a later step.

To modify the default security group to allow access to port 3333

1. Click **VPC** on the **AWS Management Console Home** page. The **Amazon VPC Console Dashboard** page appears.
2. In the left navigation pane, select **Security Groups**. The **Security Groups** page opens on the right.
3. Select the **default** security group. The details for the **default** security group appear at the bottom of the page.
4. Select the **Inbound Rules** tab. The current inbound rules appear.

   Info:

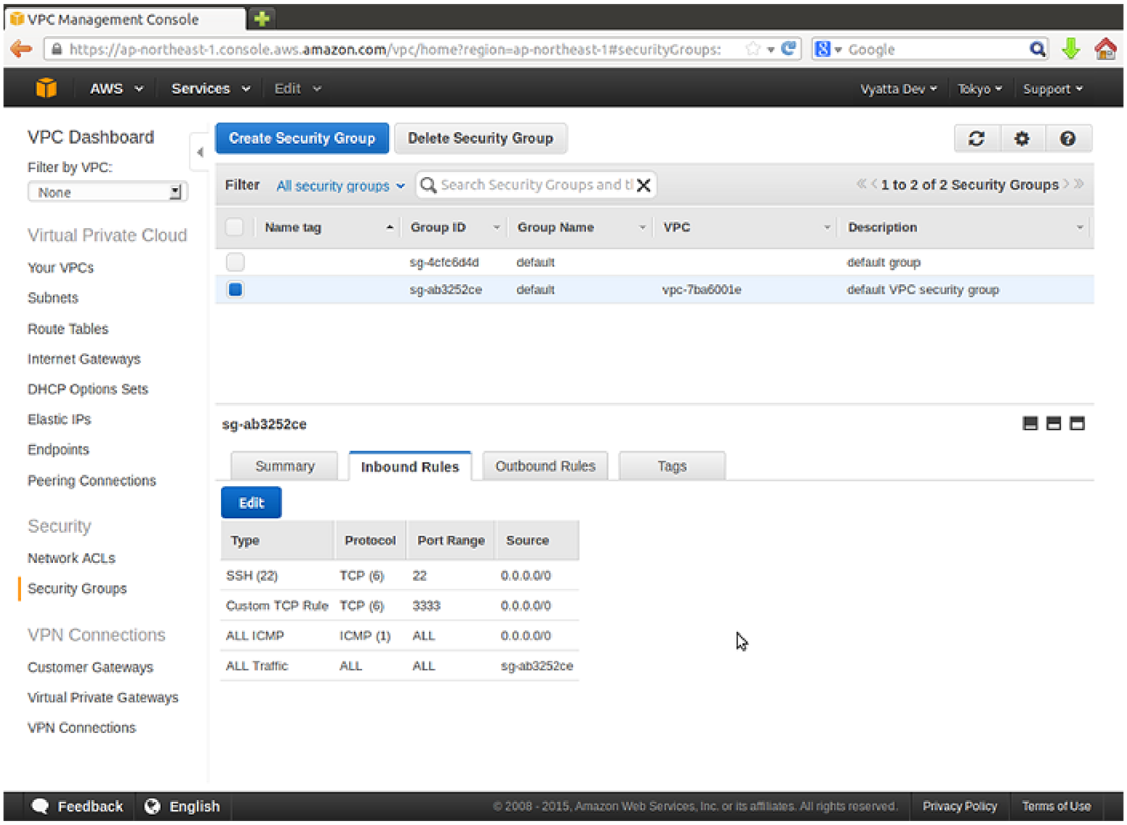


Name tag	Group ID	Group Name	VPC	Description
	sg-4cfc6d4d	default		default group
	sg-ab3252ce	default	vpc-7ba6001e (10.0.0.0/16...	default VPC security group

Type	Protocol	Port Range	Source
SSH (22)	TCP (6)	22	0.0.0.0/0
ALL ICMP	ICMP (1)	ALL	0.0.0.0/0
ALL Traffic	ALL	ALL	sg-ab3252ce

5. Select **Custom TCP rule** from the drop#down list.
6. Click on **Edit and Add another rule**.
7. In the **Port Range** field, enter **3333**. In the **Source** field, enter 0.0.0.0/0 and click **Save**. The rule appears in the rule table to the right. The security group now allows access to port 3333 from anywhere.

   Info:



	Name tag	Group ID	Group Name	VPC	Description
□		sg-4cfc6d4d	default		default group
■		sg-ab3252ce	default	vpc-7ba6001e	default VPC security group

Type	Protocol	Port Range	Source
SSH (22)	TCP (6)	22	0.0.0.0/0
Custom TCP Rule	TCP (6)	3333	0.0.0.0/0
ALL ICMP	ICMP (1)	ALL	0.0.0.0/0
ALL Traffic	ALL	ALL	sg-ab3252ce

Allow the instance to be used for NAT

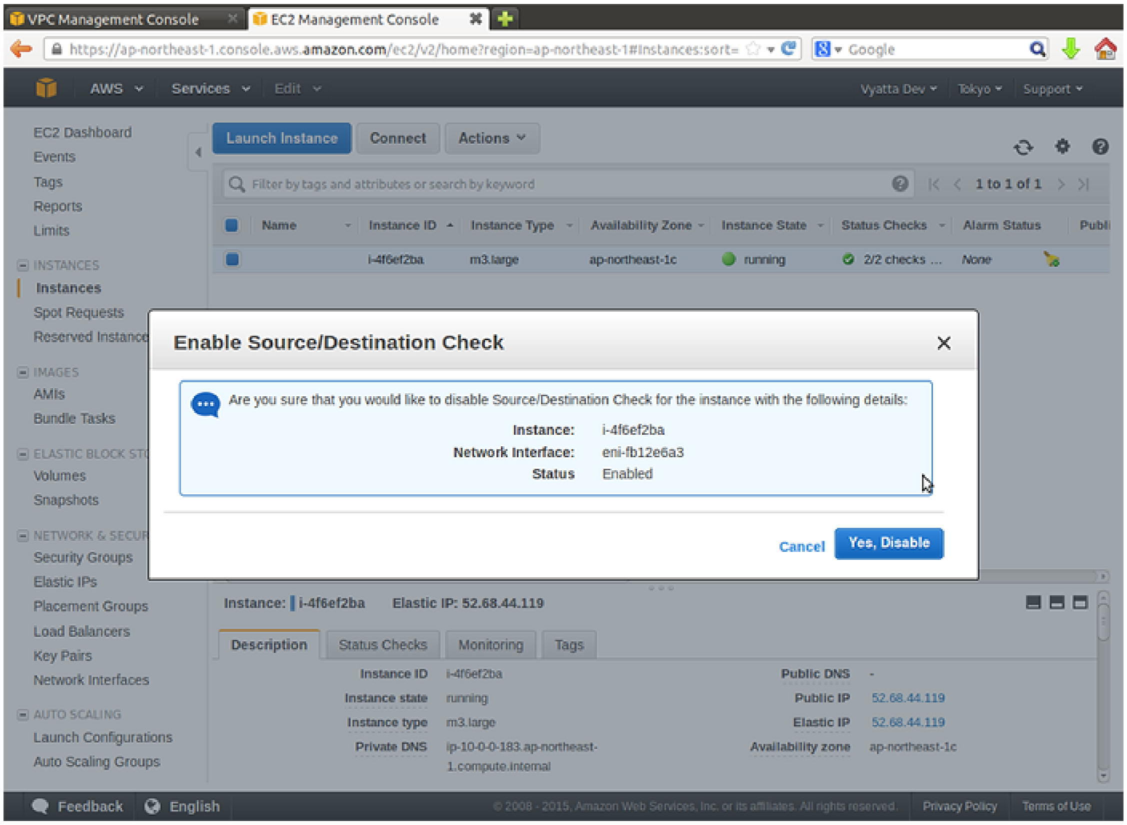
For the instance to be used as a NAT device, the checking of source and destination addresses must be disabled.

To disable the checking of source and destination addresses

1. Click **EC2** on the **AWS Management Console Home** page. The **Amazon EC2 Console Dashboard** page appears.
2. In the left navigation pane, select **Instances**. The **My Instances** page opens.
3. Right-click the row that contains the Vyatta NAT1 instance. Select **Change Source / Dest Check** from the right-click menu. The **Enable Source / Destination Check** dialog box opens.

   Info:

© 2017 AT&T Intellectual Property. All rights reserved. AT&T and Globe logo are registered trademarks of AT&T Intellectual Property.



Name	Instance ID	Instance Type	Availability Zone	Instance State	Status Checks	Alarm Status	Publi
	i-4f6ef2ba	m3.large	ap-northeast-1c	running	2/2 checks ...	None	

Enable Source/Destination Check

Are you sure that you would like to disable Source/Destination Check for the instance with the following details:

Instance: i-4f6ef2ba
Network Interface: eni-fb12e6a3
Status Enabled

Cancel   Yes, Disable

Instance: i-4f6ef2ba   Elastic IP: 52.68.44.119

Instance ID i-4f6ef2ba
Instance state running
Instance type m3.large
Private DNS ip-10-0-0-183.ap-northeast-1.compute.internal
Public DNS -
Public IP 52.68.44.119
Elastic IP 52.68.44.119
Availability zone ap-northeast-1c

4. Ensure that **Current Setting:** is set to Enabled. Click **Yes, Disable**. The instance no longer checks source and destination addresses.

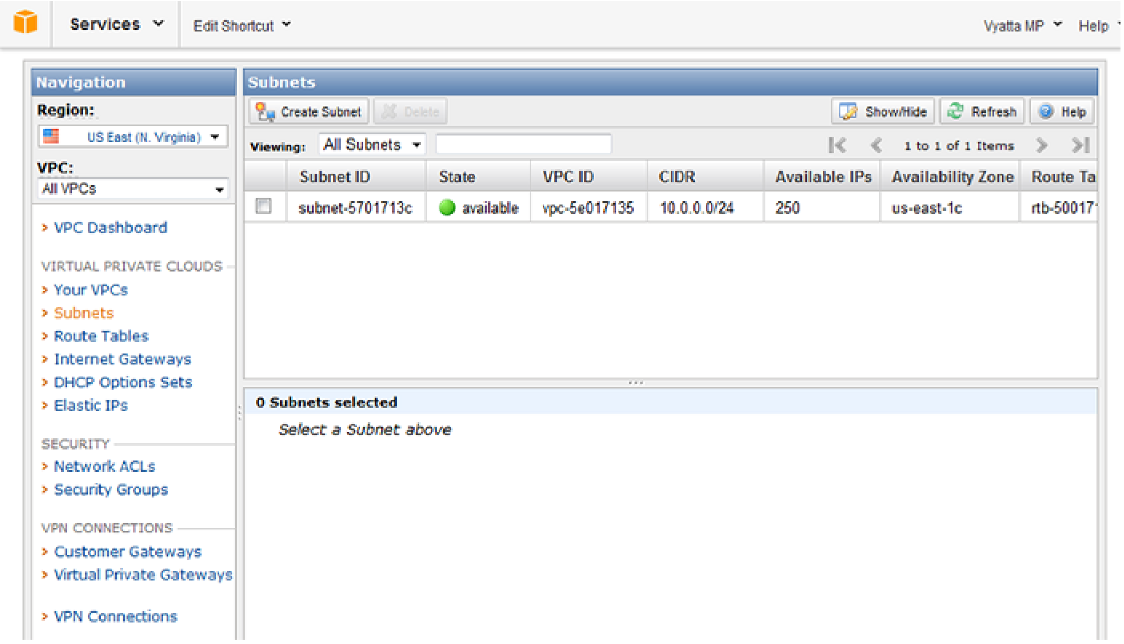
Create a private subnet

Create a new subnet within the VPC. This subnet is made private in a later step.

To create a private subnet

1. Click **VPC** on the **AWS Management Console Home** page. The **Amazon VPC Console Dashboard** page appears.
2. On the left navigation pane, select **Subnets**. The **Subnets** page opens.

   Info:



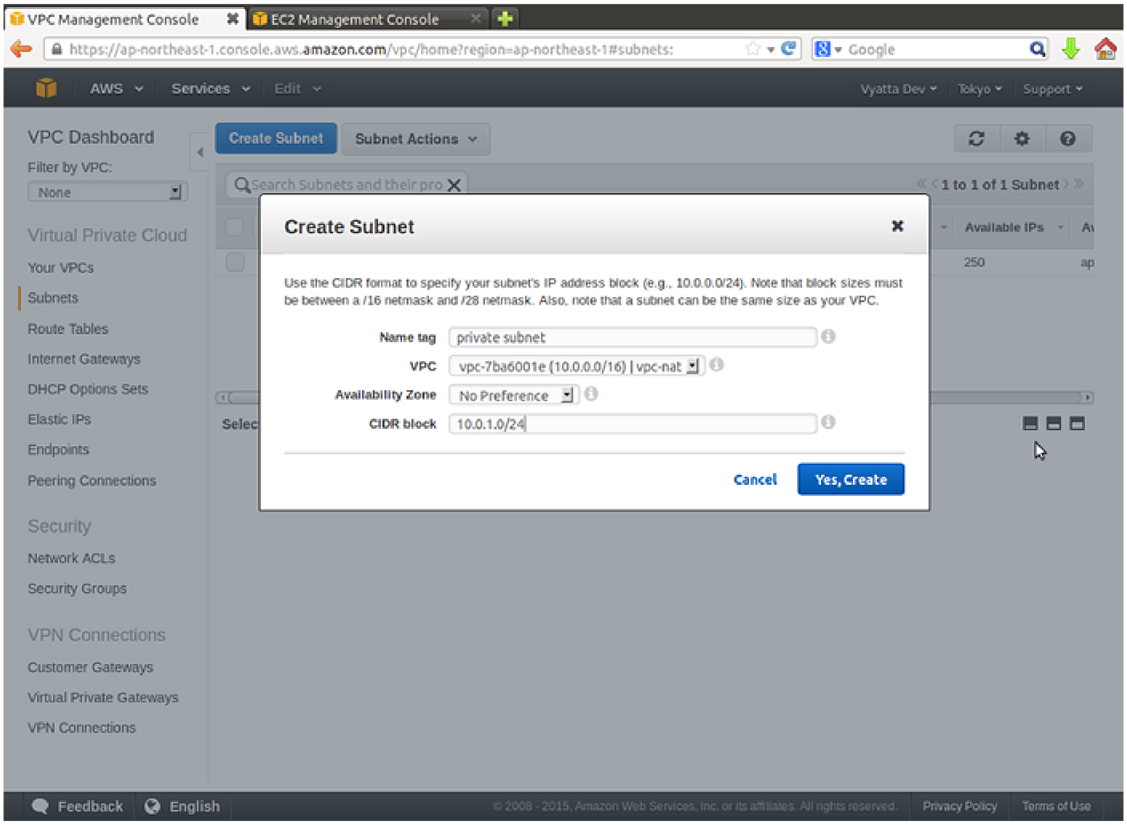
	Subnet ID	State	VPC ID	CIDR	Available IPs	Availability Zone	Route Ta
□	subnet-5701713c	● available	vpc-5e017135	10.0.0.0/24	250	us-east-1c	rtb-50017

0 Subnets selected

Select a Subnet above

3. Click **Create Subnet**. The **Create Subnet** dialog box opens.

   Info:



Create Subnet

Use the CIDR format to specify your subnet's IP address block (e.g., 10.0.0.0/24). Note that block sizes must be between a /16 netmask and /28 netmask. Also, note that a subnet can be the same size as your VPC.

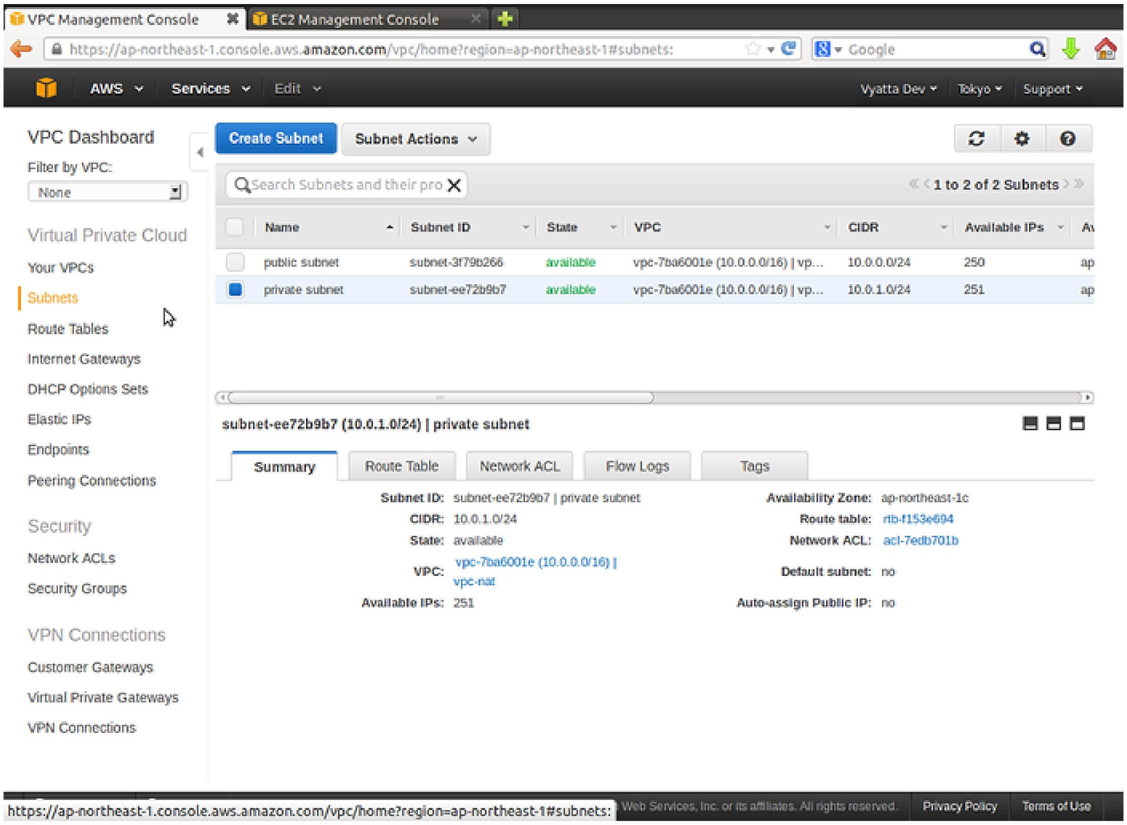
Name tag	private subnet
VPC	vpc-7ba6001e (10.0.0.0/16) | vpc-nat
Availability Zone	No Preference
CIDR block	10.0.1.0/24

4. In the CIDR block field, enter **10.0.1.0/24** and click **Yes, Create**.

   Info:

This subnet must be within the 10.0.0.0/16 range that is defined for the VPC but outside the 10.0.0.0/24 range that is configured for the public subnet.

The new subnet appears in the list of subnets.



	Name	Subnet ID	State	VPC	CIDR	Available IPs	Av
□	public subnet	subnet-3f79b266	available	vpc-7ba6001e (10.0.0.0/16) | vp...	10.0.0.0/24	250	ap
■	private subnet	subnet-ee72b9b7	available	vpc-7ba6001e (10.0.0.0/16) | vp...	10.0.1.0/24	251	ap

subnet-ee72b9b7 (10.0.1.0/24) | private subnet

Subnet ID:	subnet-ee72b9b7 | private subnet	Availability Zone:	ap-northeast-1c
CIDR:	10.0.1.0/24	Route table:	rtb-f153e694
State:	available	Network ACL:	acl-7edb701b
VPC:	vpc-7ba6001e (10.0.0.0/16) | vpc-nat	Default subnet:	no
Available IPs:	251	Auto-assign Public IP:	no

Associate a route table with the private subnet

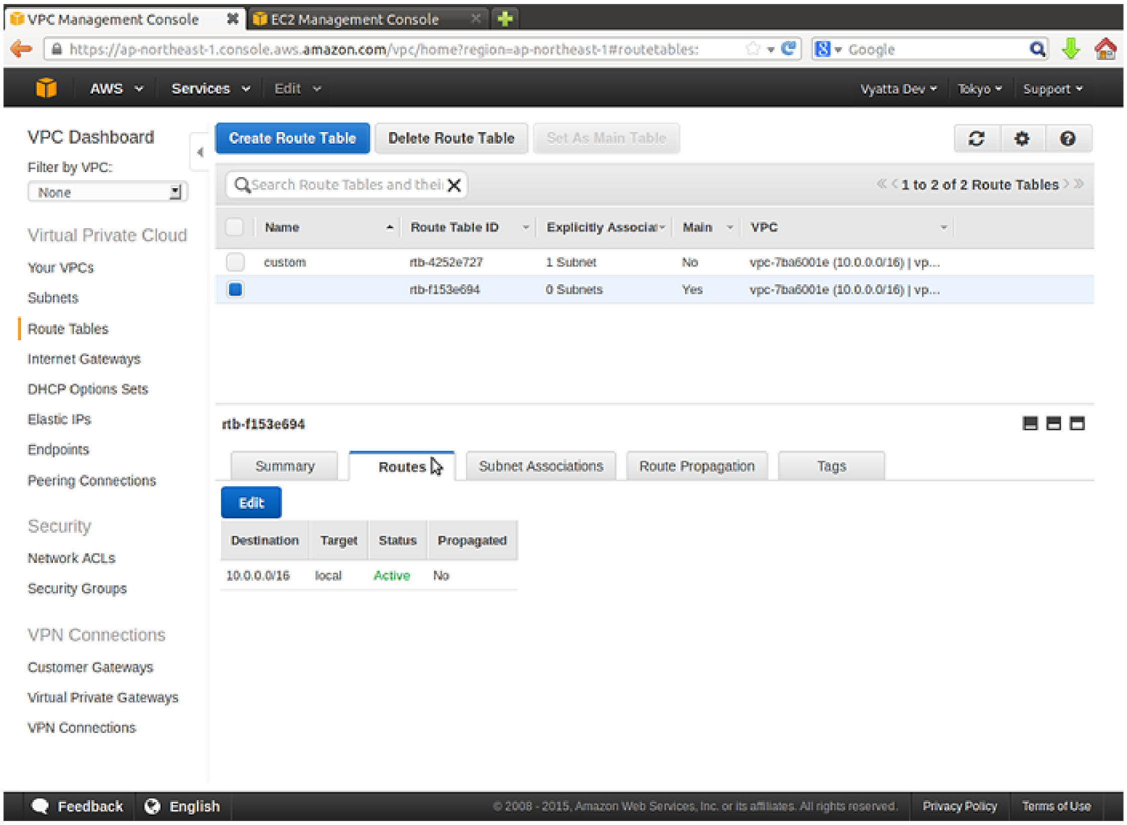
This step enables access to instances within the private subnet in the VPC, and from the private subnet to the Internet through the newly created Vyatta NAT device.

To associate a route table with the private subnet

1. Click **VPC** on the **AWS Management Console Home** page. The **Amazon VPC Console Dashboard** page appears.
2. In the left navigation pane, select **Route Tables**. The **Route Tables** page opens.

   Info:

© 2017 AT&T Intellectual Property. All rights reserved. AT&T and Globe logo are registered trademarks of AT&T Intellectual Property.



Filter by VPC: None

	Name	Route Table ID	Explicitly Associat	Main	VPC
□	custom	rtb-4252e727	1 Subnet	No	vpc-7ba6001e (10.0.0.0/16) | vp...
■		rtb-f153e694	0 Subnets	Yes	vpc-7ba6001e (10.0.0.0/16) | vp...

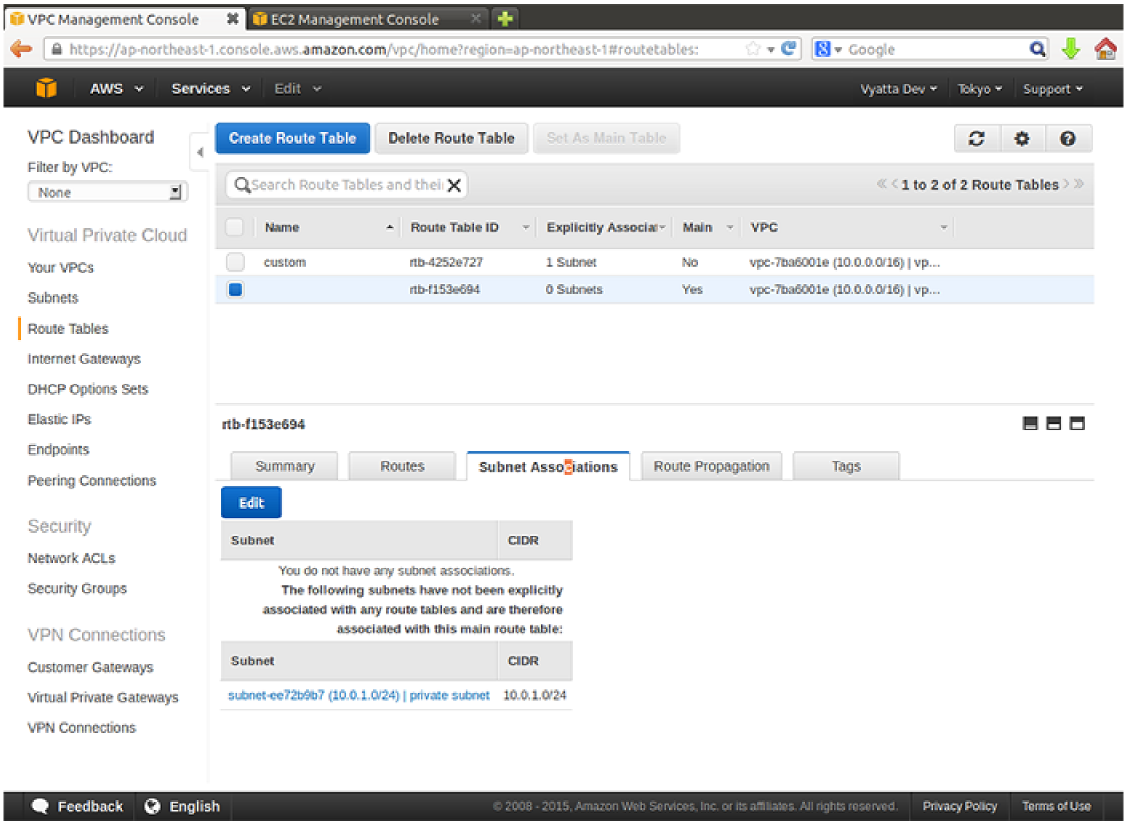
rtb-f153e694

Destination	Target	Status	Propagated
10.0.0.0/16	local	Active	No

3. Select the route table that was created when you created the new subnet and click the **Subnet Associations** tab. The **Associations** tab opens.

   Info:

© 2017 AT&T Intellectual Property. All rights reserved. AT&T and Globe logo are registered trademarks of AT&T Intellectual Property.



	Name	Route Table ID	Explicitly Associat	Main	VPC
□	custom	rtb-4252e727	1 Subnet	No	vpc-7ba6001e (10.0.0.0/16) | vp...
■		rtb-f153e694	0 Subnets	Yes	vpc-7ba6001e (10.0.0.0/16) | vp...

rtb-f153e694

Subnet	CIDR

You do not have any subnet associations.

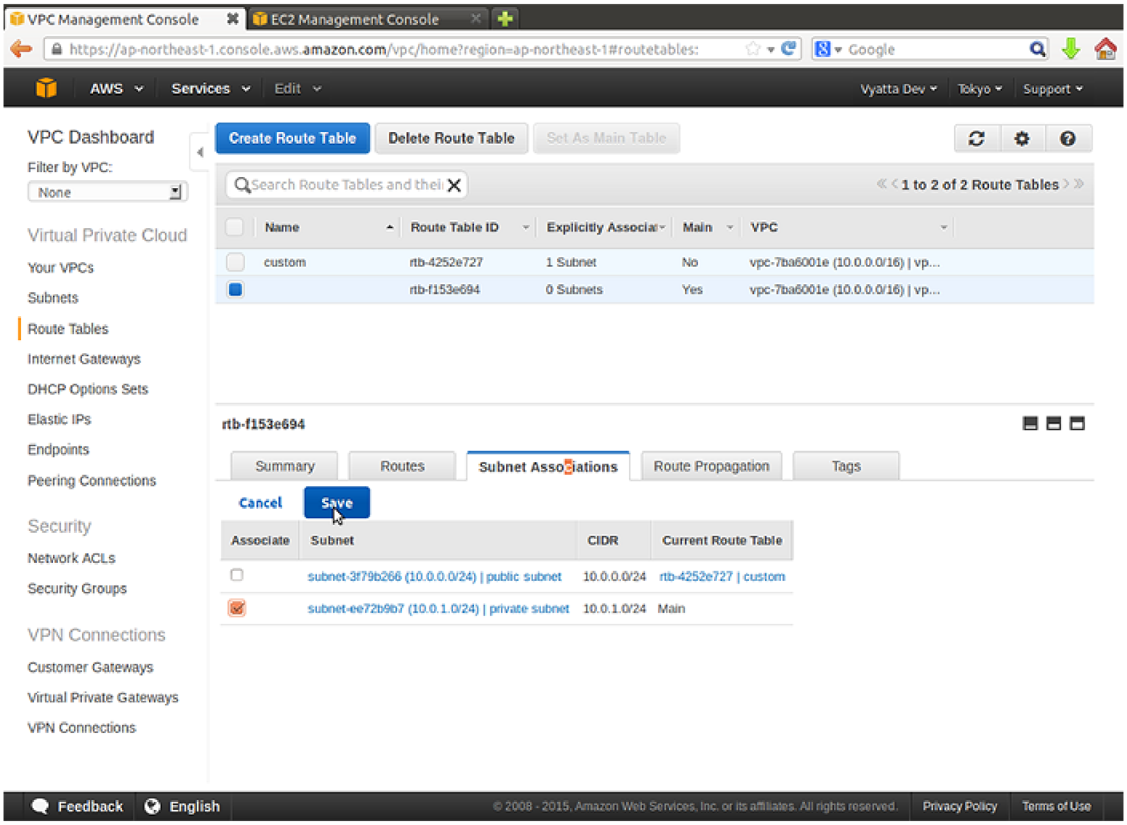
The following subnets have not been explicitly associated with any route tables and are therefore associated with this main route table:

Subnet	CIDR
subnet-ee72b9b7 (10.0.1.0/24) | private subnet	10.0.1.0/24

4. Click **Edit** to select the subnet that was just created (in this case, 10.0.1.0/24) and click **Save**.

Info:

© 2017 AT&T Intellectual Property. All rights reserved. AT&T and Globe logo are registered trademarks of AT&T Intellectual Property.



	Name	Route Table ID	Explicitly Associat	Main	VPC
□	custom	rtb-4252e727	1 Subnet	No	vpc-7ba6001e (10.0.0.0/16) | vp...
■		rtb-f153e694	0 Subnets	Yes	vpc-7ba6001e (10.0.0.0/16) | vp...

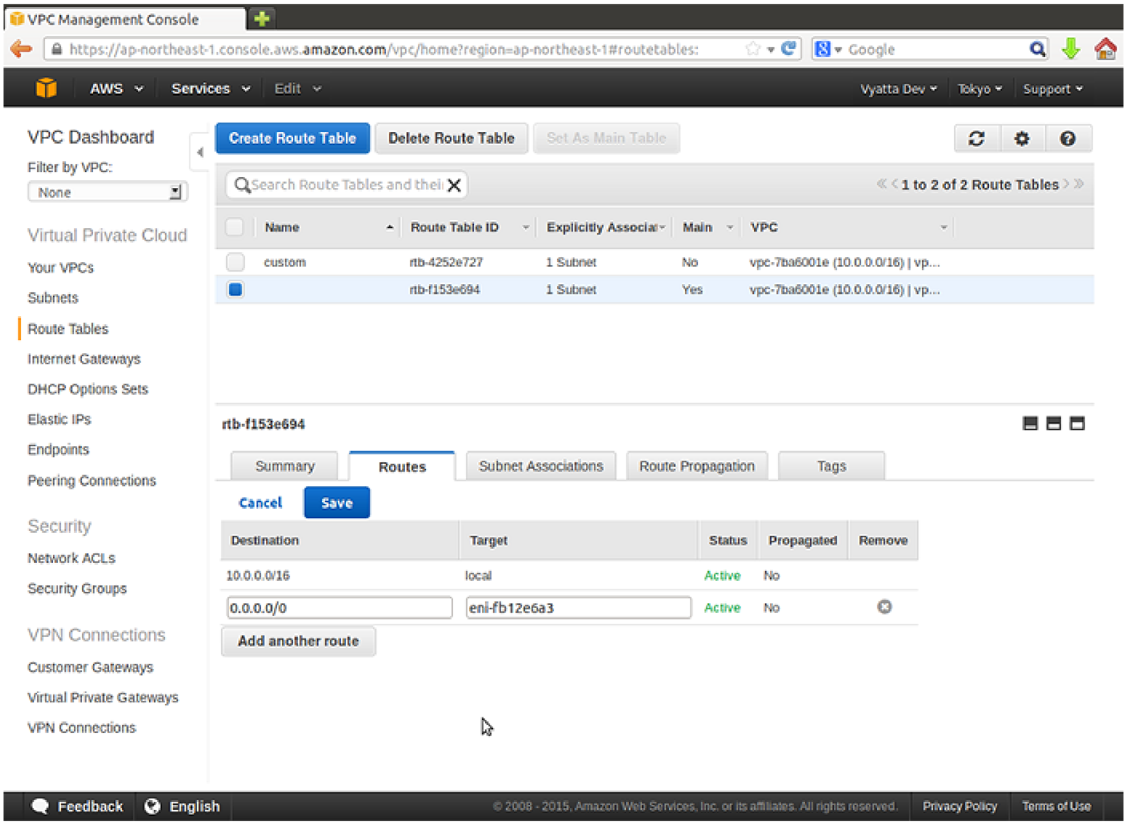
rtb-f153e694

Associate	Subnet	CIDR	Current Route Table
□	subnet-3f79b266 (10.0.0.0/24) | public subnet	10.0.0.0/24	rtb-4252e727 | custom
☑	subnet-ee72b9b7 (10.0.1.0/24) | private subnet	10.0.1.0/24	Main

5. Add a default route for the NAT interface. In this case, dp0s0 is the NAT interface, so specify the eni number for dp0s0 as shown in the following figure.

   Info:

© 2017 AT&T Intellectual Property. All rights reserved. AT&T and Globe logo are registered trademarks of AT&T Intellectual Property.



	Name	Route Table ID	Explicitly Associat	Main	VPC
□	custom	rtb-4252e727	1 Subnet	No	vpc-7ba6001e (10.0.0.0/16) | vp...
■		rtb-f153e694	1 Subnet	Yes	vpc-7ba6001e (10.0.0.0/16) | vp...

rtb-f153e694

Destination	Target	Status	Propagated	Remove
10.0.0.0/16	local	Active	No	
0.0.0.0/0	eni-fb12e6a3	Active	No	⊗

Launch an instance into the private subnet

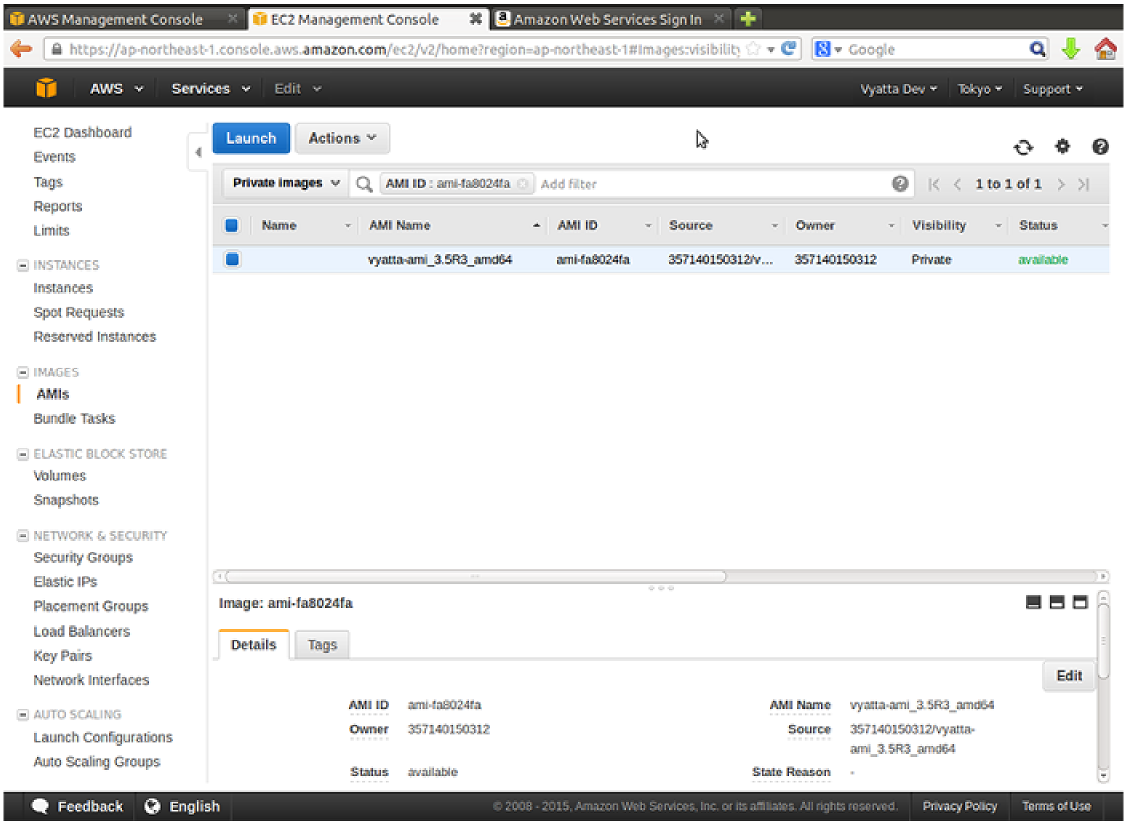
Now that the 10.0.1.0/24 private subnet has been defined, we can launch an instance into it. Although the following example shows how to launch another Vyatta AMI instance, any instance type can be launched. For this example, it is assumed that the Vyatta AMI is obtained from the EC2 Console, but it could also be obtained from the AWS Marketplace.

To launch a Vyatta AMI instance into the private subnet

1. Click **EC2** on the **AWS Management Console Home** page. The **Amazon EC2 Console Dashboard** page appears.
2. In the left navigation pane, select **AMIs**. The **Amazon Machine Images** page opens on the right.

   Info:

© 2017 AT&T Intellectual Property. All rights reserved. AT&T and Globe logo are registered trademarks of AT&T Intellectual Property.



Name	AMI Name	AMI ID	Source	Owner	Visibility	Status
	vyatta-ami_3.5R3_amd64	ami-fa8024fa	357140150312/v...	357140150312	Private	available

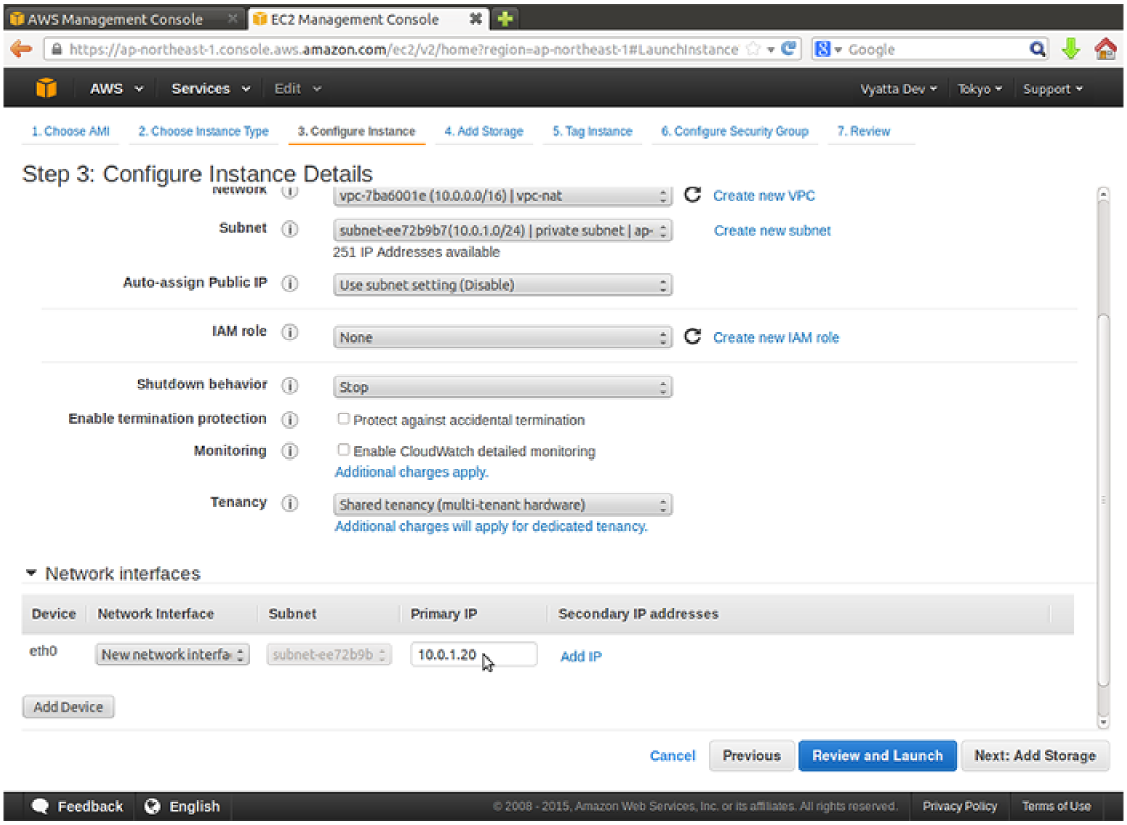
Image: ami-fa8024fa

AMI ID	ami-fa8024fa	AMI Name	vyatta-ami_3.5R3_amd64
Owner	357140150312	Source	357140150312/vyatta-ami_3.5R3_amd64
Status	available	State Reason	-

3. In the **Viewing** field, select **Private images** and specify vyatta#ami as the search string. Vyatta AMIs are listed.
4. Select a Vyatta AMI and click **Launch** at the top of the **Amazon Machine Images** page. The **Request Instances Wizard** starts at the **Instance Details** step.
5. Select **m4.large/xlarge** as the instance type and click **Configure Instance Details**.
6. On the **Configure Instance details** page, select **VPC.**
7. In the **Subnet** field, select the 10.0.1.0/24 subnet to which to attach the instance.

Info:

© 2017 AT&T Intellectual Property. All rights reserved. AT&T and Globe logo are registered trademarks of AT&T Intellectual Property.



Step 3: Configure Instance Details

Network	vpc-7ba6001e (10.0.0.0/16) | vpc-nat	Create new VPC
Subnet	subnet-ee72b9b7(10.0.1.0/24) | private subnet | ap- 251 IP Addresses available	Create new subnet
Auto-assign Public IP	Use subnet setting (Disable)	
IAM role	None	Create new IAM role
Shutdown behavior	Stop	
Enable termination protection	□ Protect against accidental termination	
Monitoring	□ Enable CloudWatch detailed monitoring Additional charges apply.	
Tenancy	Shared tenancy (multi-tenant hardware) Additional charges will apply for dedicated tenancy.	

Network interfaces

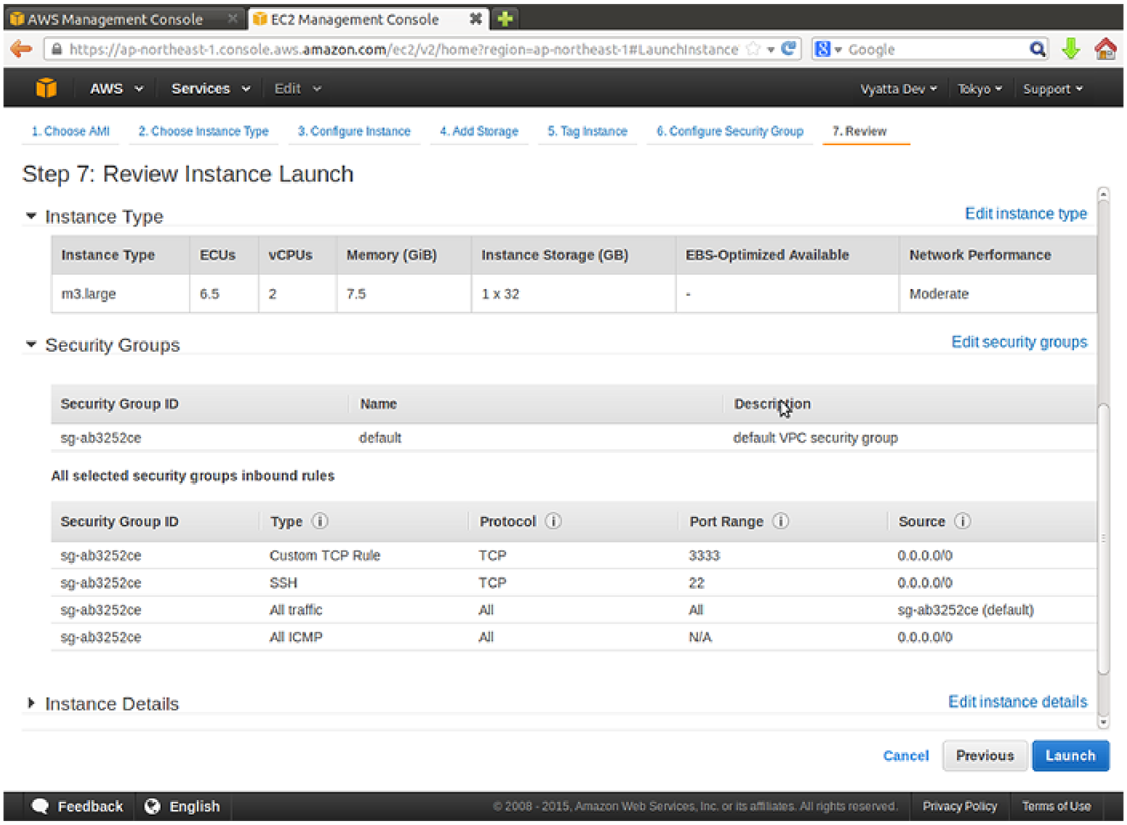
Device	Network Interface	Subnet	Primary IP	Secondary IP addresses
eth0	New network interfa	subnet-ee72b9b	10.0.1.20	Add IP

8. In the **IP Address** field, enter **10.0.1.20** and click **Add Storage**. The **Storage Device Configuration** page opens.
9. If you want to change the size of the storage device that is associated with the instance, click **Edit**. In most cases, this is not necessary. Click **Tag Instance**. You can tag EC2 resources, if required. Click **Configure Security Group**.

   Info:

10. Select an existing security group or create a new one. Click **Review and Launch**.

    Info:



Step 7: Review Instance Launch

Instance Type

Instance Type	ECUs	vCPUs	Memory (GiB)	Instance Storage (GB)	EBS-Optimized Available	Network Performance
m3.large	6.5	2	7.5	1 x 32	-	Moderate

Security Groups

Security Group ID	Name	Description
sg-ab3252ce	default	default VPC security group

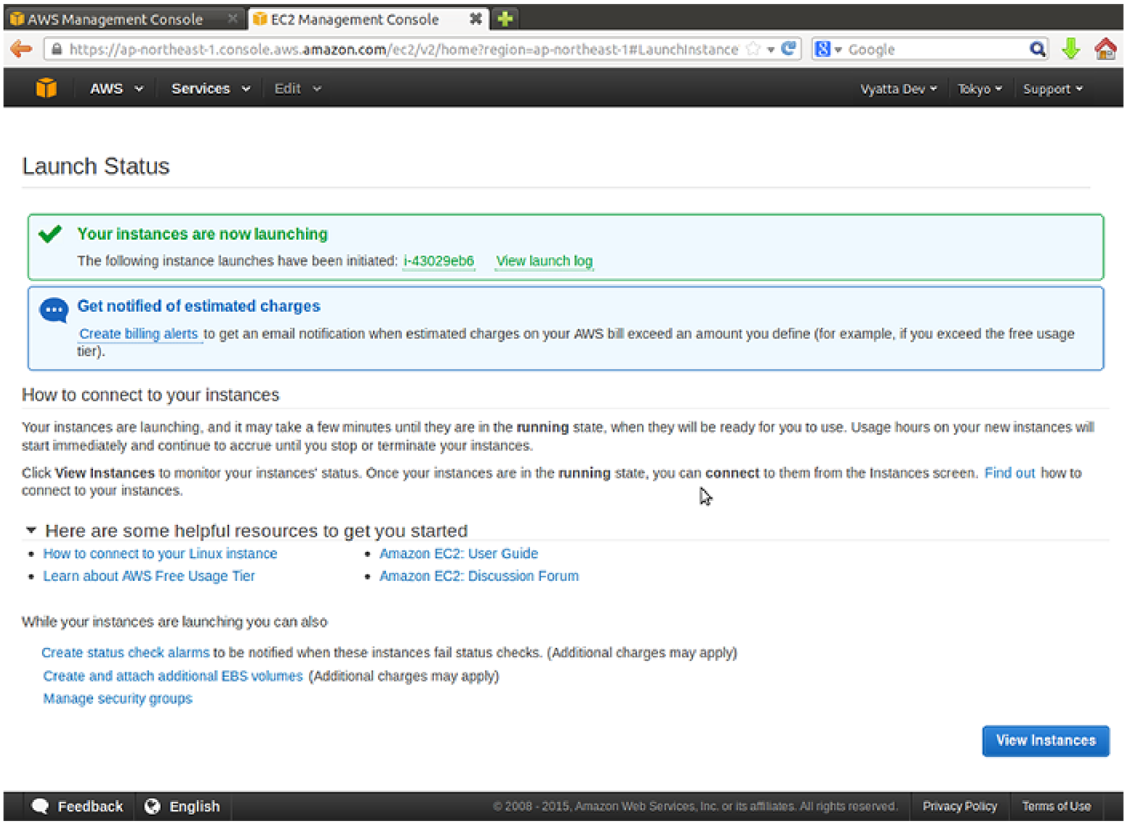
All selected security groups inbound rules

Security Group ID	Type	Protocol	Port Range	Source
sg-ab3252ce	Custom TCP Rule	TCP	3333	0.0.0.0/0
sg-ab3252ce	SSH	TCP	22	0.0.0.0/0
sg-ab3252ce	All traffic	All	All	sg-ab3252ce (default)
sg-ab3252ce	All ICMP	All	N/A	0.0.0.0/0

Instance Details

11. Select **Choose from your existing Key Pairs** and select an existing key pair from the **Your existing Key Pairs** drop#down list.
12. Click **Launch Instances**

    Info:



AWS Management Console
EC2 Management Console
https://ap-northeast-1.console.aws.amazon.com/ec2/v2/home?region=ap-northeast-1#LaunchInstance
Google
AWS
Services
Edit
Vyatta Dev
Tokyo
Support

Launch Status

Your instances are now launching

The following instance launches have been initiated: i-43029eb6 View launch log

Get notified of estimated charges

Create billing alerts to get an email notification when estimated charges on your AWS bill exceed an amount you define (for example, if you exceed the free usage tier).

How to connect to your instances

Your instances are launching, and it may take a few minutes until they are in the **running** state, when they will be ready for you to use. Usage hours on your new instances will start immediately and continue to accrue until you stop or terminate your instances.

Click **View Instances** to monitor your instances' status. Once your instances are in the **running** state, you can **connect** to them from the Instances screen. Find out how to connect to your instances.

Here are some helpful resources to get you started

- How to connect to your Linux instance
- Learn about AWS Free Usage Tier
- Amazon EC2: User Guide
- Amazon EC2: Discussion Forum

While your instances are launching you can also

Create status check alarms to be notified when these instances fail status checks. (Additional charges may apply)

Create and attach additional EBS volumes (Additional charges may apply)

Manage security groups

View Instances
Feedback
English
© 2008 - 2015, Amazon Web Services, Inc. or its affiliates. All rights reserved.
Privacy Policy
Terms of Use

13. To view the status of the newly launched instance, select **Instances** on the left navigation pane within the **EC2** tab.

Access the private instance remotely

Because the default security group is associated with the instance, remote SSH connections are allowed through to it.

To access the instance remotely by using SSH

1. On a remote machine, open an SSH session. As the destination, use the Elastic IP address that you associated with the Vyatta NAT instance. Enter **3333** as the port.

   Info:

   Note: On Linux and UNIX systems, use the `ssh` command. On Windows machines use a program such as putty for SSH access.

2. The Vyatta NAT device has been configured to translate any connections to port 3333 to address 10.0.1.20 port 22. This connection is routed to the instance that is created within the private subnet.

   Info:

3. Use the ssh private key to connect to the VM for the vyatta user.

Verify the instance is working as expected

After you are logged on to the system, enter the following commands to confirm that it is working as expected.

To confirm that the instance is working as expected

1. Confirm the IP address that is associated with the Ethernet interface.

   Info:

© 2017 AT&T Intellectual Property. All rights reserved. AT&T and Globe logo are registered trademarks of AT&T Intellectual Property.

```
vyatta@vyatta:~$ show interfaces
Codes: S - State, L - Link, u - Up, D - Down, A - Admin Down
Interface        IP Address                        S/L  Description
---------        ----------                        ---  -----------
dp0s0            10.0.1.20/24                      u/u
vyatta@vyatta:~$
```

2. Confirm that the instance has access to the Internet by using `ping` (press <Ctrl>+c to stop the output).

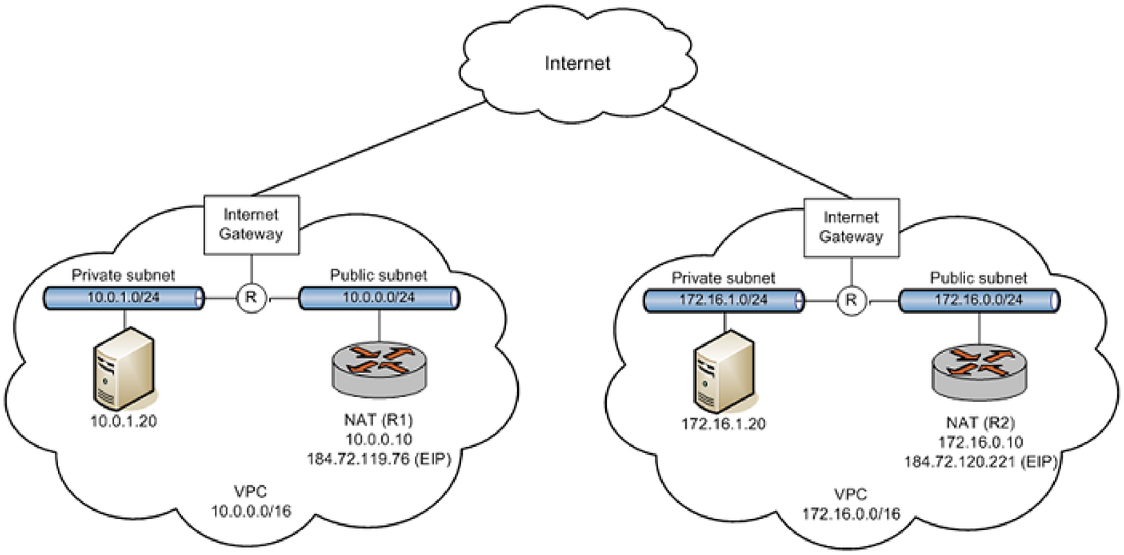
   Info:

```
vyatta@vyatta:~$ ping www.vyatta.com

PING www.vyatta.com (76.74.103.45) 56(84) bytes of data.
64 bytes from www.vyatta.com (76.74.103.45): icmp_req=1 ttl=46 time=74.4 ms
64 bytes from www.vyatta.com (76.74.103.45): icmp_req=2 ttl=46 time=74.5 ms
^C
--- www.vyatta.com ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 74.492/74.502/74.513/0.273 ms
vyatta@vyatta:~$ ^C
vyatta@vyatta:~$
```

Creating a site-to-site IPsec VPN connection

In this example, a site-to-site IPsec VPN connection is created between the NAT devices in separate VPCs. In the example, it is assumed that Vyatta NAT instances and instances within private subnets have been created within the VPCs according to the steps in Creating a NAT device *(page 20)*. The following diagram shows the configuration.



To allow inbound Internet Key Exchange (IKE), Encapsulating Security Payload (ESP), and IPsec NAT-T, add three rules to the default VPC security group in each VPC. The first inbound rule (for IKE) allows UDP traffic on port 500 from any source (0.0.0.0/0). The second inbound rule (for ESP) is a Custom protocol rule and allows IP protocol 50 traffic from any source (0.0.0.0/0). The third inbound rule (for IPsec NAT-T) allows UDP traffic on port 4500 from any source (0.0.0.0/0). Refer to Modify the default security group *(page 22)* as a reference.

To provide an IPsec VPN endpoint on the R1 NAT device, configure the device as follows:

```
vyatta@vyatta# show security vpn

vpn {
```

© 2017 AT&T Intellectual Property. All rights reserved. AT&T and Globe logo are registered trademarks of AT&T Intellectual Property.

```
        ipsec {
                esp-group ESP-1W {
                        lifetime 1800
                        proposal 1 {
                                encryption aes256
                        }
                        proposal 2 {
                                encryption 3des
                                hash md5
                        }
                }
                ike-group IKE-1W {
                        lifetime 3600
                        proposal 1 {
                                encryption aes256
                        }
                        proposal 2
                }
                nat-networks {
                        allowed-network 0.0.0.0/0 {
                                exclude 10.0.0.0/16
                        }
                }
                nat-traversal enable
                site-to-site {
                        peer 52.64.93.132 {
                                authentication {
                                        id @router1
                                        pre-shared-secret test123
                                        remote-id @router2
                                }
                                default-esp-group ESP-1W
                                ike-group IKE-1W
                                local-address 10.0.0.183
                                tunnel 1 {
                                        local {
                                                prefix 10.0.0.0/16
                                        }
                                        remote {
                                                prefix 172.16.0.0/16
                                        }
                                }
                        }
                }
        }
 }
```

To provide an IPsec VPN endpoint on the R2 NAT device, configure the device as follows:

```
vyatta@vyatta# show security vpn

vpn {
        ipsec {
                esp-group ESP-1E {
                        lifetime 1800
                        proposal 1 {
                                encryption aes256
                        }
                        proposal 2 {
                                encryption 3des
                                hash md5
                        }
                }
                ike-group IKE-1E {
                        lifetime 3600
                        proposal 1 {
                                encryption aes256
                        }
                        proposal 2
                }
                nat-networks {
                        allowed-network 0.0.0.0/0 {
                                exclude 172.16.0.0/16
                        }
                }
                nat-traversal enable
                site-to-site {
                        peer 52.68.44.119 {
                                authentication {
                                        id @router2
                                        pre-shared-secret test123
                                        remote-id @router1
                                }
                                default-esp-group ESP-1E
                                ike-group IKE-1E
                                local-address 172.16.0.10
                                tunnel 1 {
                                        local {
                                                prefix 172.16.0.0/16
                                        }
                                        remote {
                                                prefix 10.0.0.0/16
                                        }
                                }
                        }
                }
        }
 }
[edit]
```

Test the configuration by pinging a device in one private subnet (10.0.1.20) from a device in the other private subnet (172.16.1.20).

```
vyatta@vyatta:~$ ping 10.0.1.20

PING 10.0.1.20 (10.0.1.20) 56(84) bytes of data.
64 bytes from 10.0.1.20: icmp_req=1 ttl=64 time=0.439 ms
64 bytes from 10.0.1.20: icmp_req=2 ttl=64 time=0.572 ms
64 bytes from 10.0.1.20: icmp_req=3 ttl=64 time=0.430 ms
64 bytes from 10.0.1.20: icmp_req=4 ttl=64 time=0.448 ms
^C
--- 10.0.1.20 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 2997ms
rtt min/avg/max/mdev = 0.430/0.472/0.572/0.059 ms
vyatta@vyatta:~$
```

While this example shows a site-to-site IPsec VPN connection between sites in two different VPCs, the sites can also be located in non-VPC locations (for example, a branch office or a data center).

For further information on IPsec VPN configuration, refer to AT&T Vyatta Network Operating System IPsec Site-to-Site VPN Configuration Guide.

© 2017 AT&T Intellectual Property. All rights reserved. AT&T and Globe logo are registered trademarks of AT&T Intellectual Property.

Upgrading the System

This chapter explains how to upgrade AT&T Vyatta vRouter software on an AT&T Vyatta Amazon Machine Image (AMI) in Amazon Web Services (AWS).

Release-specific upgrade information

Your system may have special upgrade considerations, depending on the release.

For release-specific upgrade information, and to ensure that configuration information is correctly preserved across upgrades, consult the release notes for your release.

Before upgrading

Before upgrading, save your existing configuration file for reference. Your configuration file is named `config.boot` and is located in the `/config` directory.

Upgrading an AT&T Vyatta AMI

To upgrade the AT&T Vyatta AMI

1. Save your current system configuration (`/config`) to a separate location on your network.
2. Using the new Vyatta AMI, create a new Vyatta virtual machine in your AWS environment. Use the instructions given in Chapter 1: Installing the System, starting in "Obtaining and Launching the Vyatta AMI" on page 9 *(page 11)*.
3. Perform initial configuration of the new virtual machine and test the installation to verify connectivity on the network.
4. Shut down the old system so that it does not conflict with the new system.
5. Load the configuration you saved onto the new Vyatta virtual machine.
6. Reboot the system by using the `reboot` command. The system restarts with the new configuration.

   Info:

© 2017 AT&T Intellectual Property. All rights reserved. AT&T and Globe logo are registered trademarks of AT&T Intellectual Property.

List of Acronyms

Acronym	Description
ACL	access control list
ADSL	Asymmetric Digital Subscriber Line
AH	Authentication Header
AMI	Amazon Machine Image
API	Application Programming Interface
AS	autonomous system
ARP	Address Resolution Protocol
AWS	Amazon Web Services
BGP	Border Gateway Protocol
BIOS	Basic Input Output System
BPDU	Bridge Protocol Data Unit
CA	certificate authority
CCMP	AES in counter mode with CBC-MAC
CHAP	Challenge Handshake Authentication Protocol
CLI	command-line interface
DDNS	dynamic DNS
DHCP	Dynamic Host Configuration Protocol
DHCPv6	Dynamic Host Configuration Protocol version 6
DLCI	data-link connection identifier
DMI	desktop management interface
DMVPN	dynamic multipoint VPN
DMZ	demilitarized zone
DN	distinguished name
DNS	Domain Name System
DSCP	Differentiated Services Code Point
DSL	Digital Subscriber Line
eBGP	external BGP
EBS	Amazon Elastic Block Storage
EC2	Amazon Elastic Compute Cloud
EGP	Exterior Gateway Protocol
ECMP	equal-cost multipath
ESP	Encapsulating Security Payload
FIB	Forwarding Information Base
FTP	File Transfer Protocol
GRE	Generic Routing Encapsulation
HDLC	High-Level Data Link Control
I/O	Input/Output
ICMP	Internet Control Message Protocol
IDS	Intrusion Detection System
IEEE	Institute of Electrical and Electronics Engineers

© 2017 AT&T Intellectual Property. All rights reserved. AT&T and Globe logo are registered trademarks of AT&T Intellectual Property.

Acronym	Description
IGMP	Internet Group Management Protocol
IGP	Interior Gateway Protocol
IPS	Intrusion Protection System
IKE	Internet Key Exchange
IP	Internet Protocol
IPOA	IP over ATM
IPsec	IP Security
IPv4	IP Version 4
IPv6	IP Version 6
ISAKMP	Internet Security Association and Key Management Protocol
ISM	Internet Standard Multicast
ISP	Internet Service Provider
KVM	Kernel-Based Virtual Machine
L2TP	Layer 2 Tunneling Protocol
LACP	Link Aggregation Control Protocol
LAN	local area network
LDAP	Lightweight Directory Access Protocol
LLDP	Link Layer Discovery Protocol
MAC	medium access control
mGRE	multipoint GRE
MIB	Management Information Base
MLD	Multicast Listener Discovery
MLPPP	multilink PPP
MRRU	maximum received reconstructed unit
MTU	maximum transmission unit
NAT	Network Address Translation
NBMA	Non-Broadcast Multi-Access
ND	Neighbor Discovery
NHRP	Next Hop Resolution Protocol
NIC	network interface card
NTP	Network Time Protocol
OSPF	Open Shortest Path First
OSPFv2	OSPF Version 2
OSPFv3	OSPF Version 3
PAM	Pluggable Authentication Module
PAP	Password Authentication Protocol
PAT	Port Address Translation
PCI	peripheral component interconnect
PIM	Protocol Independent Multicast
PIM-DM	PIM Dense Mode
PIM-SM	PIM Sparse Mode
PKI	Public Key Infrastructure
PPP	Point-to-Point Protocol
PPPoA	PPP over ATM

© 2017 AT&T Intellectual Property. All rights reserved. AT&T and Globe logo are registered trademarks of AT&T Intellectual Property.

Acronym	Description
PPPoE	PPP over Ethernet
PPTP	Point-to-Point Tunneling Protocol
PTMU	Path Maximum Transfer Unit
PVC	permanent virtual circuit
QoS	quality of service
RADIUS	Remote Authentication Dial-In User Service
RHEL	Red Hat Enterprise Linux
RIB	Routing Information Base
RIP	Routing Information Protocol
RIPng	RIP next generation
RP	Rendezvous Point
RPF	Reverse Path Forwarding
RSA	Rivest, Shamir, and Adleman
Rx	receive
S3	Amazon Simple Storage Service
SLAAC	Stateless Address Auto-Configuration
SNMP	Simple Network Management Protocol
SMTP	Simple Mail Transfer Protocol
SONET	Synchronous Optical Network
SPT	Shortest Path Tree
SSH	Secure Shell
SSID	Service Set Identifier
SSM	Source-Specific Multicast
STP	Spanning Tree Protocol
TACACS+	Terminal Access Controller Access Control System Plus
TBF	Token Bucket Filter
TCP	Transmission Control Protocol
TKIP	Temporal Key Integrity Protocol
ToS	Type of Service
TSS	TCP Maximum Segment Size
Tx	transmit
UDP	User Datagram Protocol
VHD	virtual hard disk
vif	virtual interface
VLAN	virtual LAN
VPC	Amazon virtual private cloud
VPN	virtual private network
VRRP	Virtual Router Redundancy Protocol
WAN	wide area network
WAP	wireless access point
WPA	Wired Protected Access

© 2017 AT&T Intellectual Property. All rights reserved. AT&T and Globe logo are registered trademarks of AT&T Intellectual Property.