FortiMail™ AWS Deployment Guide

FORTINET DOCUMENT LIBRARY

http://docs.fortinet.com

FORTINET VIDEO GUIDE

http://video.fortinet.com

FORTINET BLOG

https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT

https://support.fortinet.com

FORTINET COOKBOOK

http://cookbook.fortinet.com

FORTINET TRAINING SERVICES

http://www.fortinet.com/training

FORTIGUARD CENTER

http://www.fortiguard.com

END USER LICENSE AGREEMENT

http://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK

Email: techdocs@fortinet.com

May 19, 2016

Table of Contents

Regions and Availability Zones

Amazon EC2 Key Pairs

Detailed VPC Diagram

Additional info and links

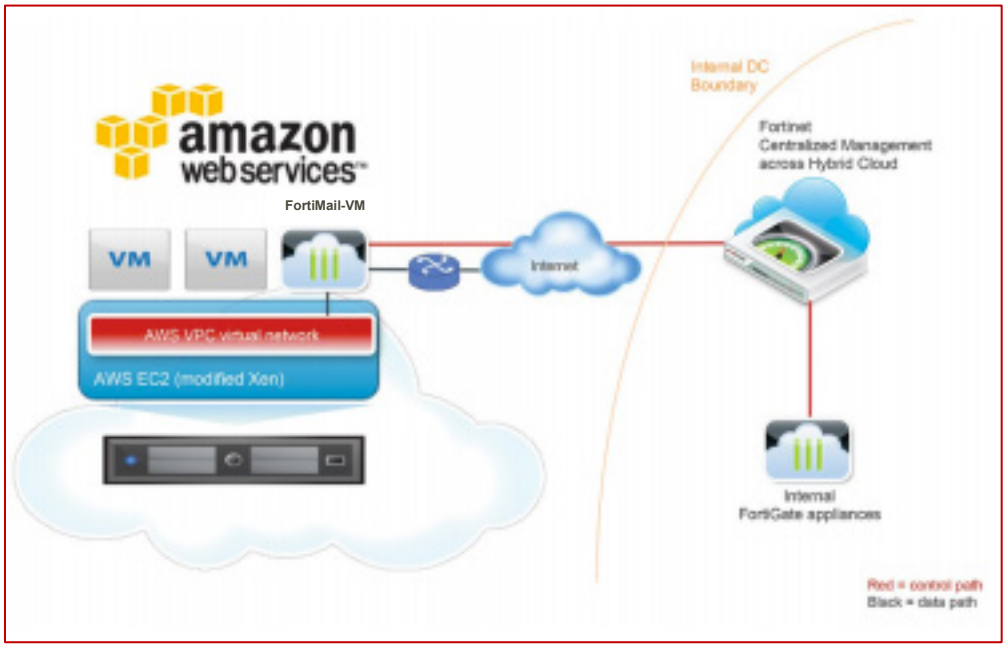
Overview

This document is design to be a quick start walk-though in setting up a virtual FortiMail device utilizing the AWS services.

Amazon Virtual Private Cloud (Amazon VPC)

Amazon VPC lets you provision a logically isolated section of the Amazon Web Services (AWS) Cloud where you can launch AWS resources in a virtual network that you define. You have complete control over your virtual networking environment, including selection of your own IP address range, creation of subnets, and configuration of route tables and network gateways. You can also create a Hardware Virtual Private Network (VPN) connection between your corporate datacenter and your VPC and leverage the AWS cloud as an extension of your corporate datacenter.

You can easily customize the network configuration for your Amazon VPC. For example, you can create a public-facing subnet for your web servers that have access to the Internet, and place your backend systems such as databases or application servers in a private-facing subnet with no Internet access. You can leverage multiple layers of security, including security groups and network access control lists, to help control access to Amazon EC2 instances in each subnet.



Components of Amazon VPC

Amazon VPC is comprised of a variety of objects that will be familiar to customers with existing networks:

- **A Virtual Private Cloud (VPC):** a logically isolated virtual network in the AWS cloud. You define a VPC's IP address space from a range you select.
- **Subnet:** a segment of a VPC's IP address range where you can place groups of isolated resources.
- **Internet Gateway:** the Amazon VPC side of a connection to the public Internet.
- **NAT Instance:** An EC2 instance that provides Port Address Translation for non-EIP instances to access the Internet via the Internet Gateway.
- **Hardware VPN Connection:** a hardware-based VPN connection between your Amazon VPC and your datacenter, home network, or co-location facility.
- **Virtual Private Gateway:** the Amazon VPC side of a VPN Connection.
- **Customer Gateway:** Your side of a VPN Connection.
- **Router:** Routers interconnect Subnets and direct traffic between Internet Gateways, Virtual Private Gateways, NAT instances and Subnets.
- **Peering Connection:** A peering connection enables you to route traffic via private IP addresses between two peered VPCs.

How do instances in a VPC access the Internet?

Elastic IP addresses (EIPs) give instances in the VPC the ability to both directly communicate outbound to the Internet and to receive unsolicited inbound traffic from the Internet (e.g., web servers)

How do instances without EIPs access the Internet?

Instances without EIPs can access the Internet in one of two ways:

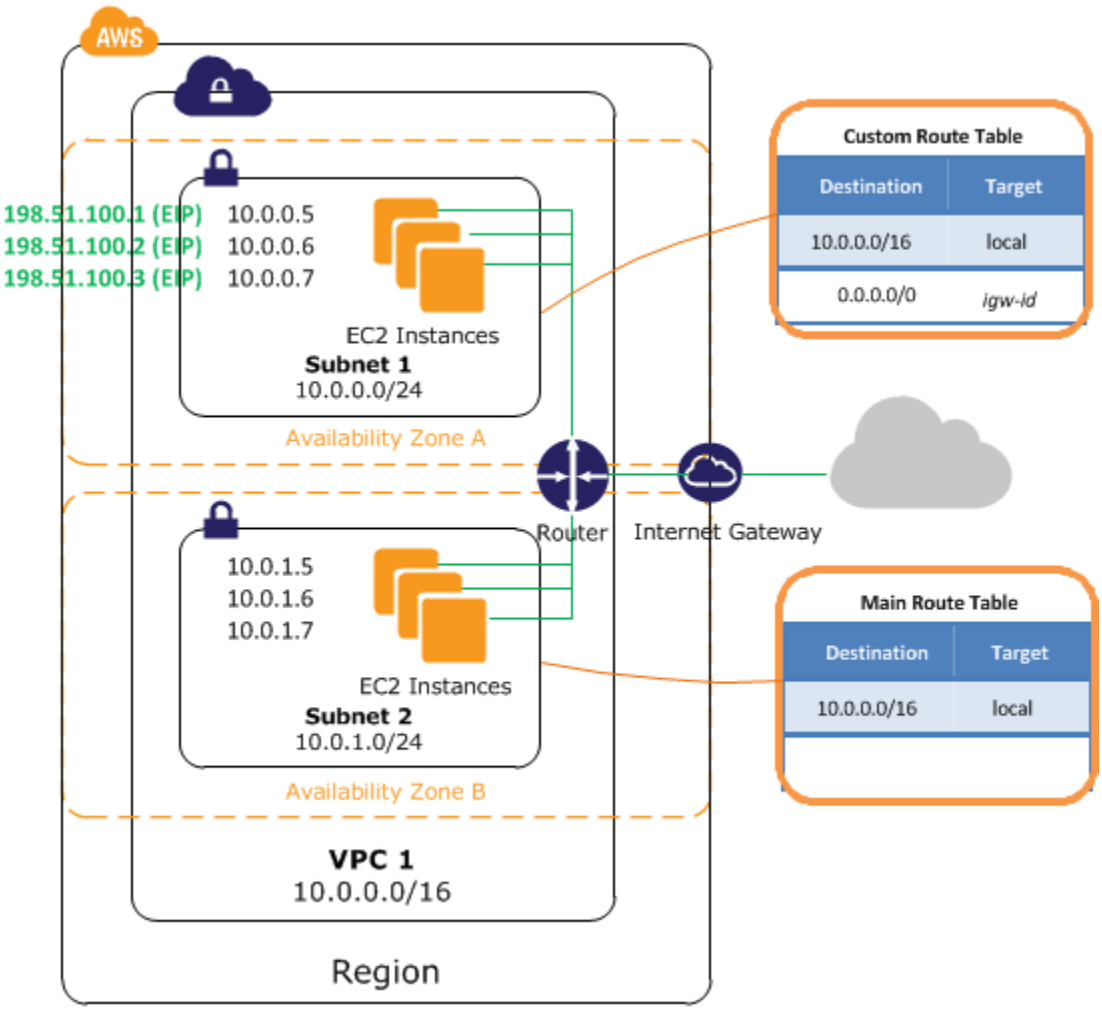
Instances without EIPs can route their traffic through a NAT instance to access the Internet. These instances use the EIP of the NAT instance to traverse the Internet. The NAT instance allows outbound communication but doesn't enable machines on the Internet to initiate a connection to the privately addressed machines using NAT, and

For VPCs with a Hardware VPN connection, instances can route their Internet traffic down the Virtual Private Gateway to your existing datacenter. From there, it can access the Internet via your existing egress points and network security/monitoring devices.

Network Information

The following diagram shows the default network design for a Public and Private VPC. We will be replacing much of the router functionality with the FortiMail as described in the previous diagram.

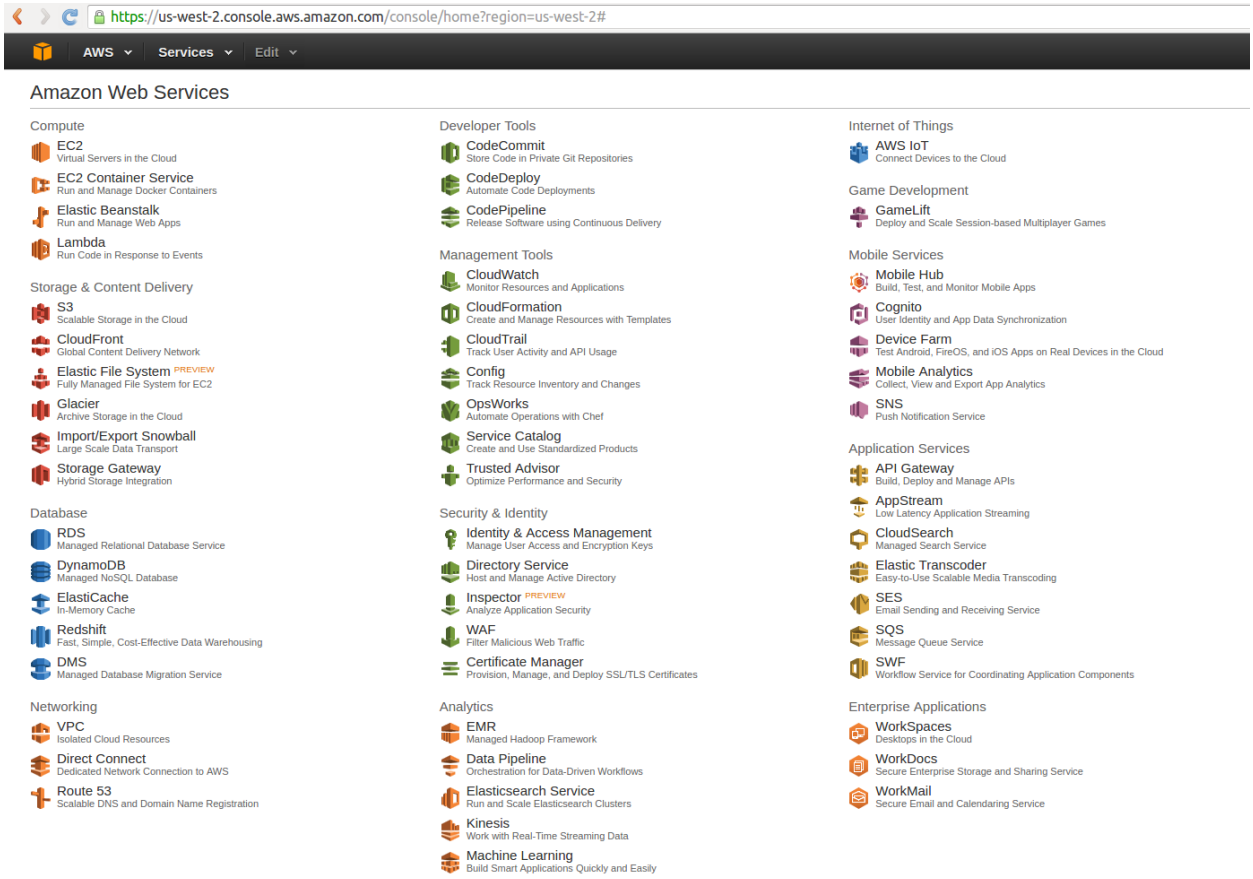
- VPC Subnet – 10.0.0.0/16
- Public Subnet - 10.0.0.0/24
- Private Subnet – 10.0.1.0/24



Basic AWS Network Setup

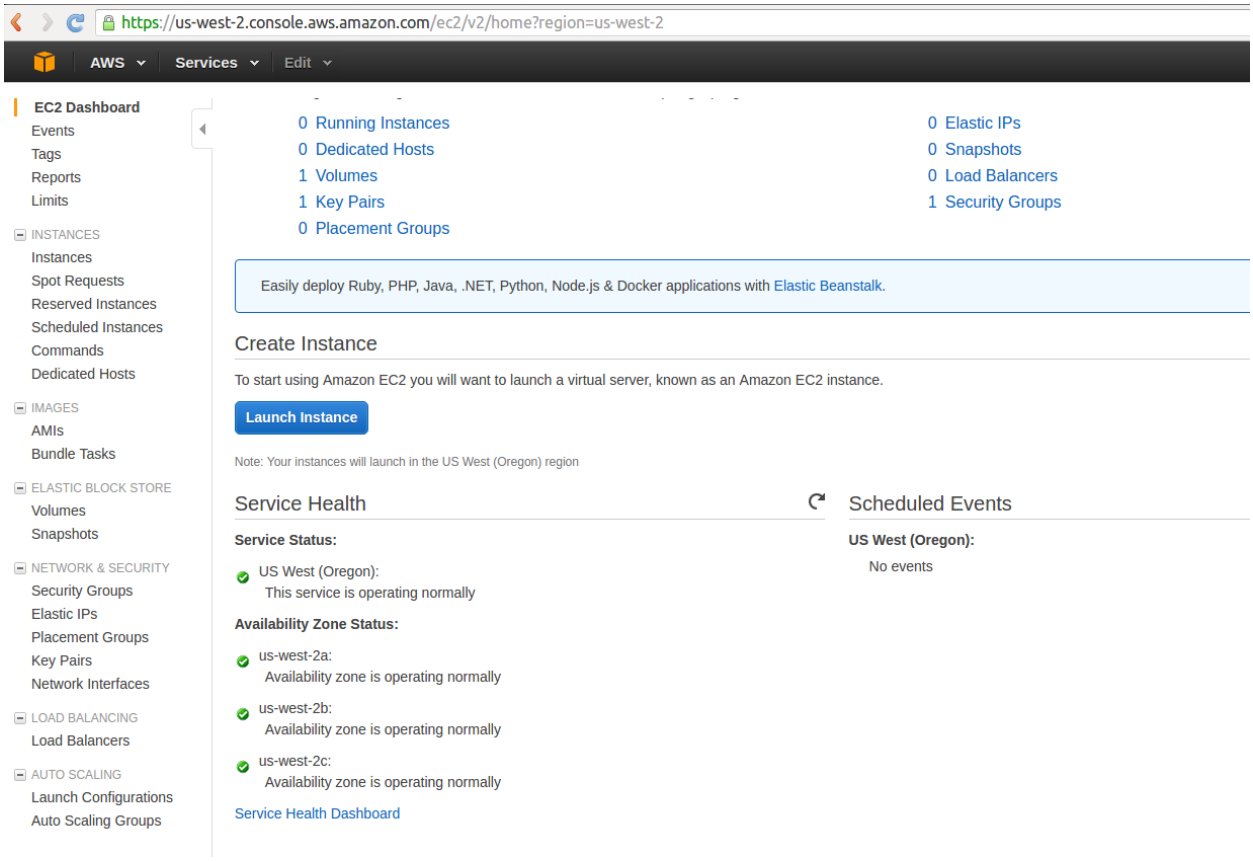
Step 1 – Setting up your AWS account

You will need to provide billing information to setup an AWS account. Once you have completed the basic account setup you will be presented with the AWS console.



Step 2 – Create a Virtual Private Cloud (VPC)

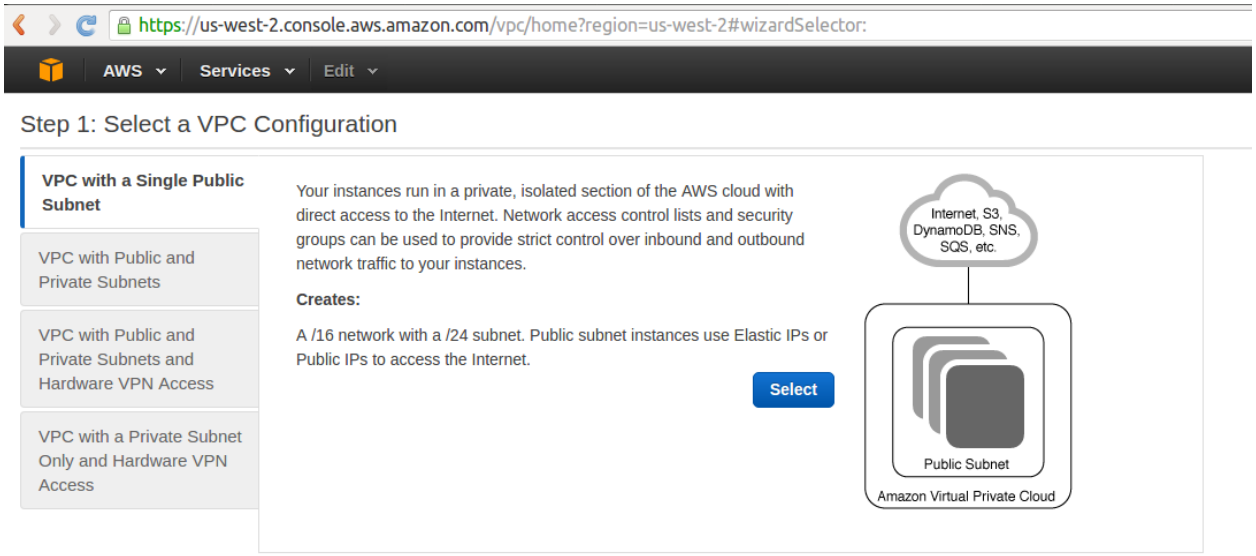
To allow VM instances access to more than one interface you need to create a VPC (virtual private cloud). You need to change dashboards to VPC and for our purpose start the VPC wizard.

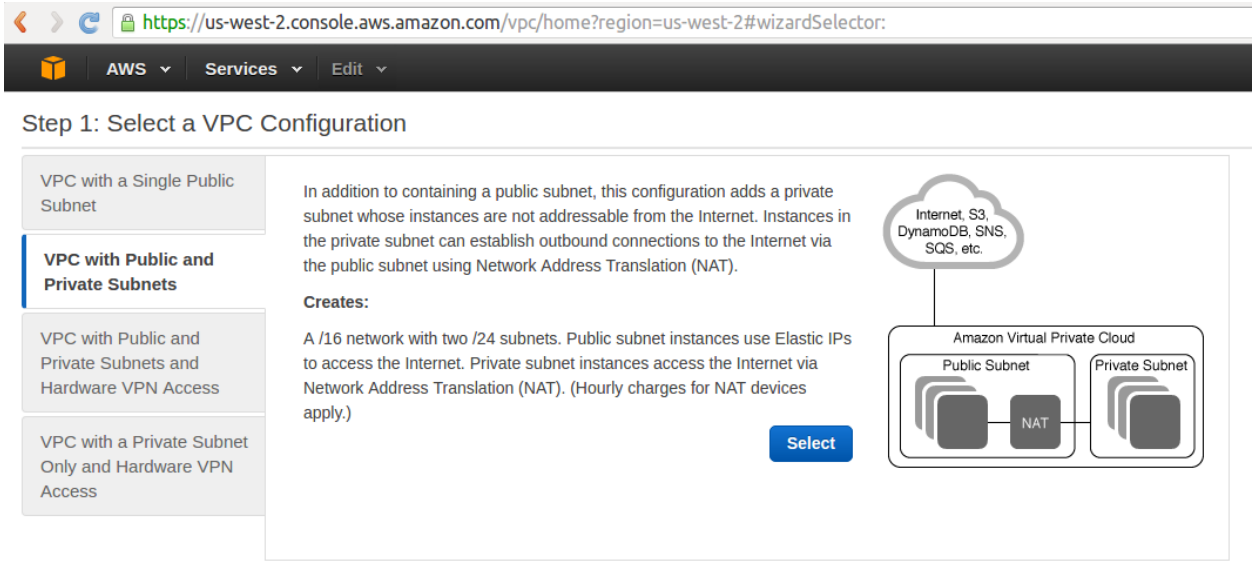


It is important to note that like most multi-tenant environments AWS reserves the first 5 IP address of each network that is created for its own router / firewall and DHCP / DNS servers.

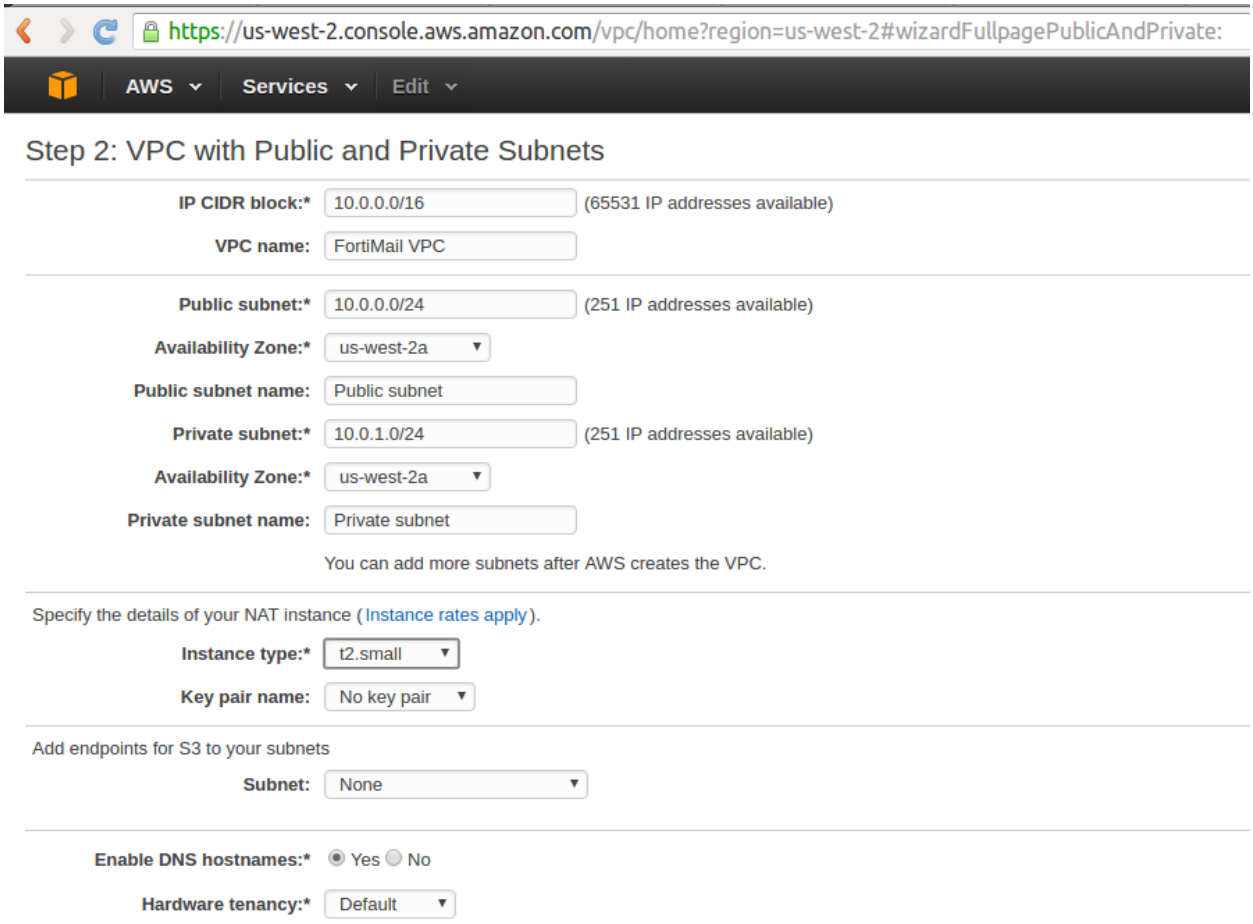
Step 2.1 – VPC Wizard

This next section is a visual walk-through of the VPC wizard. Select the Public and Private subnet option.

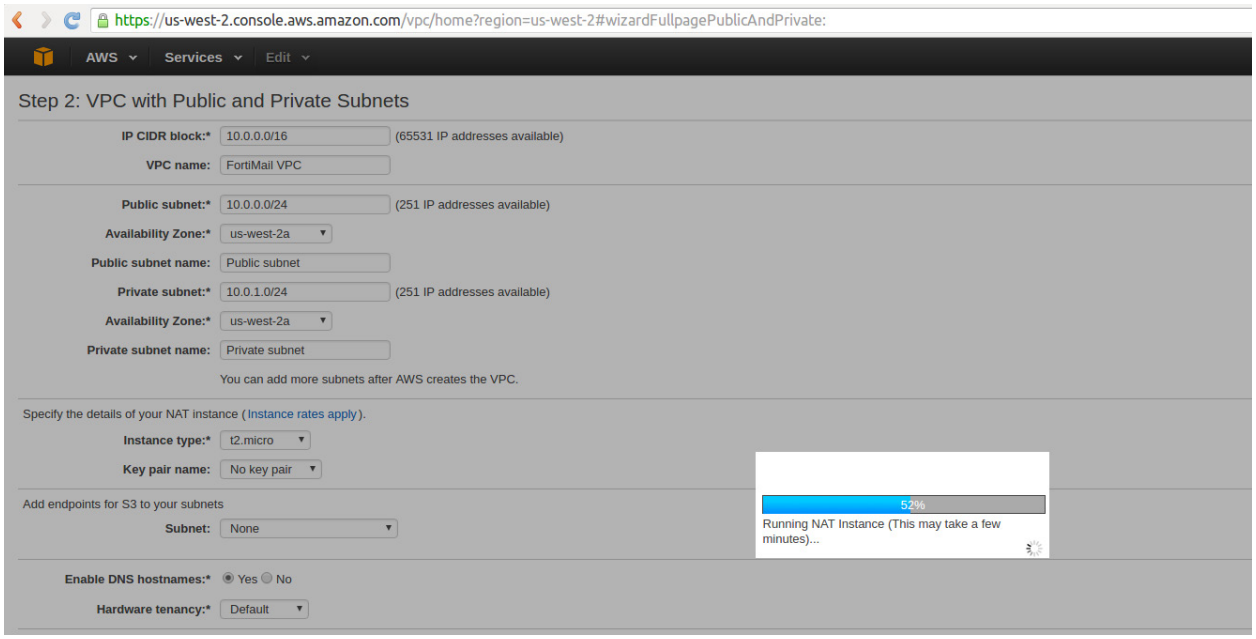




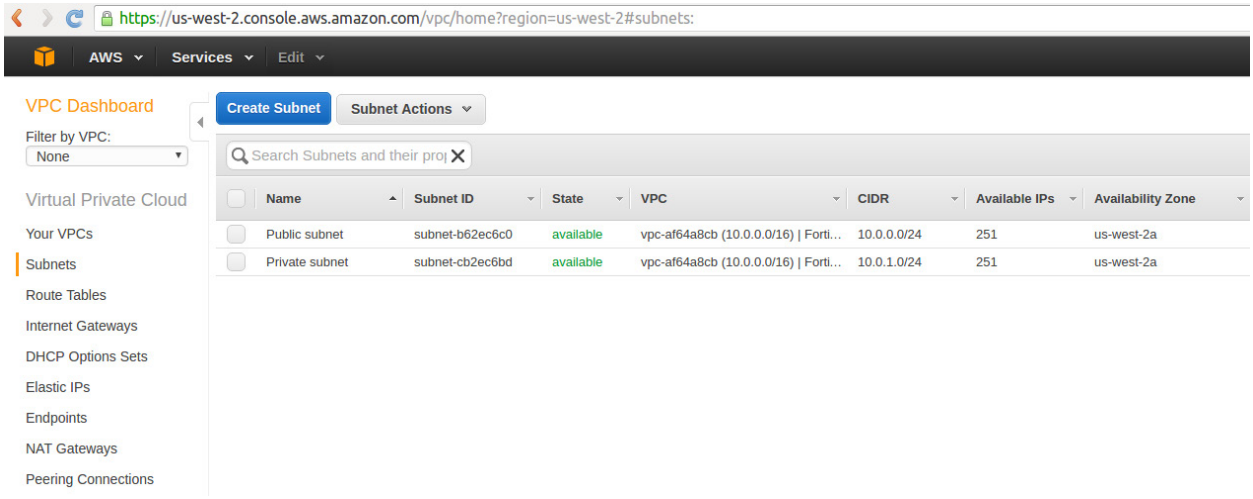
One item to double check on step 2 of the VPC wizard is to make sure that both subnets are in the *same availability zone*. Please see the Appendix for more information on availability zones.



Once you have verified the network setting, click create VPC and you will see the screen below.

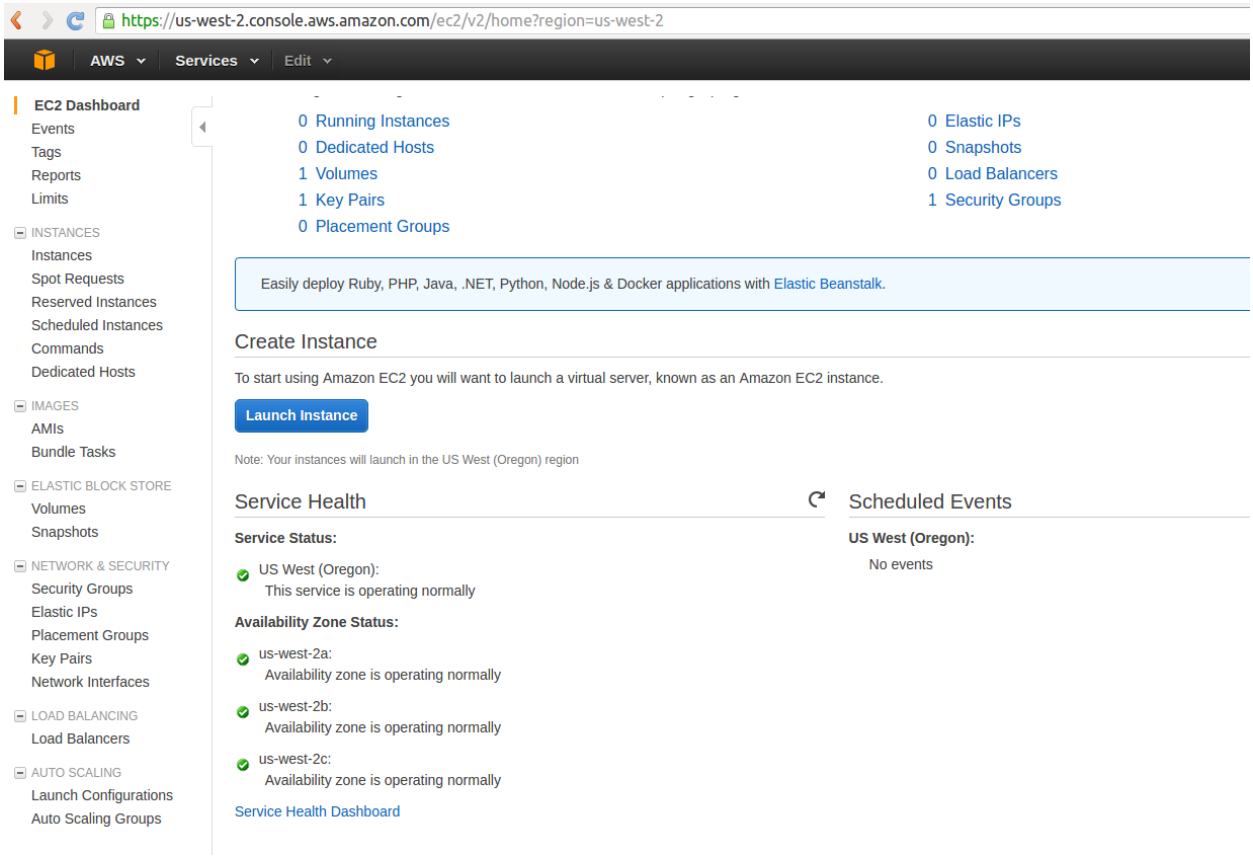


When the VPC setup has been completed you can review subnet and routing information on the VPC Dashboard.

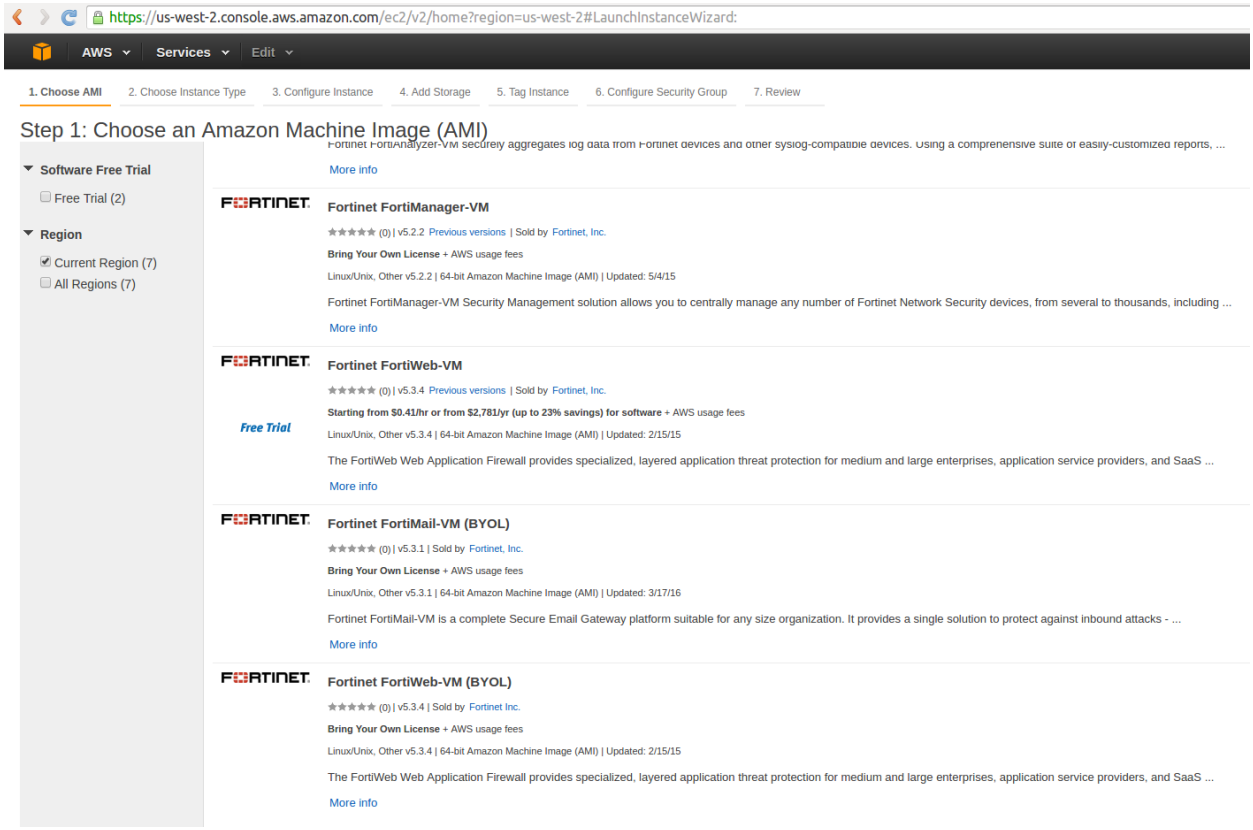


Step 3 – EC2 Launching virtual machines

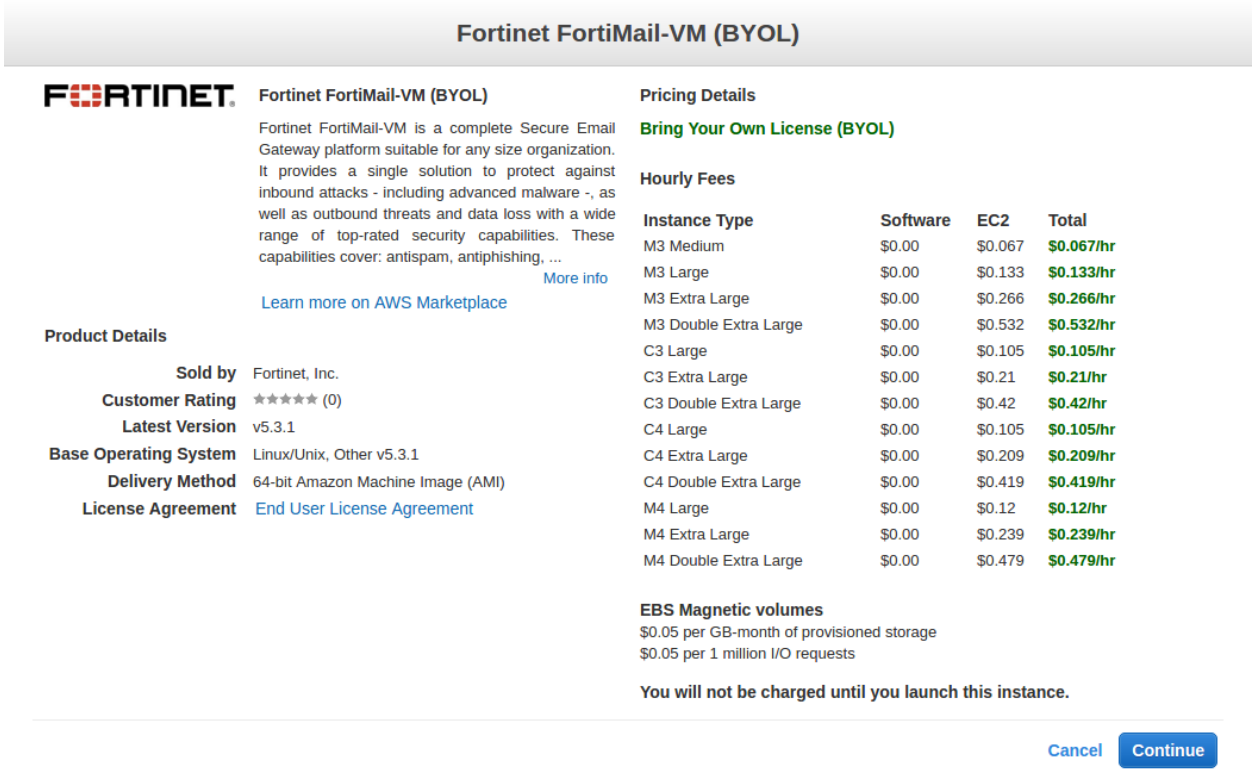
Change dashboards to the EC2 dashboard. To save time, it is normally faster to get the VM provisioning started while setting up the network. Click Launch Instance on this screen.



Step 3. 1 – Choosing an AMI

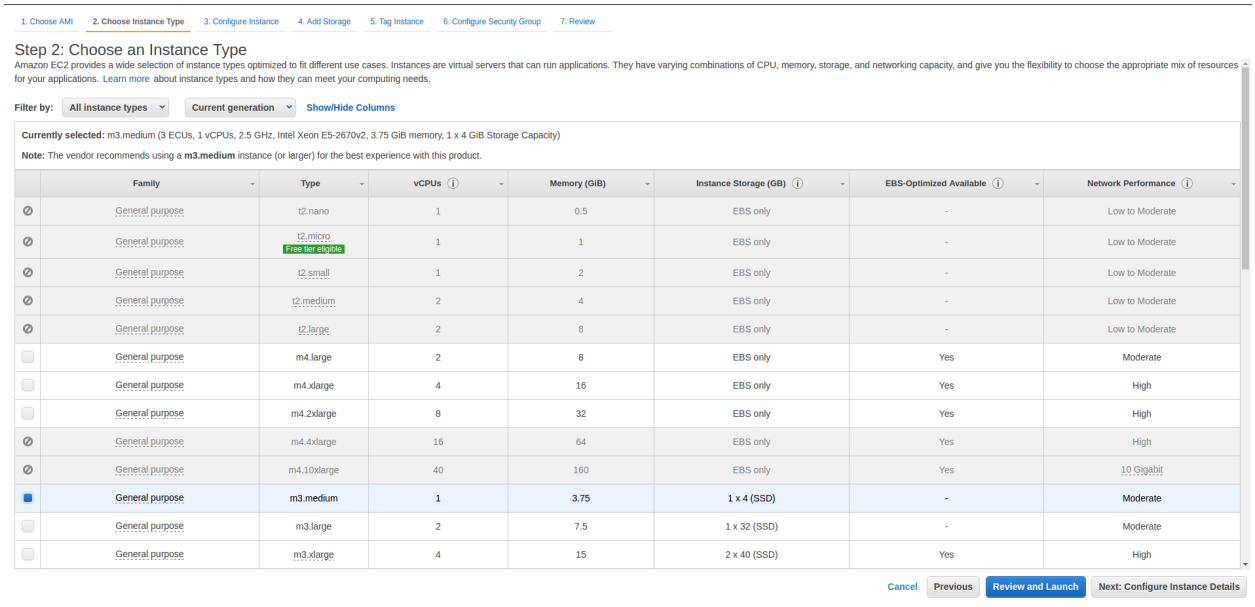


For this guide we have chosen the Bring your Own License version of the FortiMail VM.



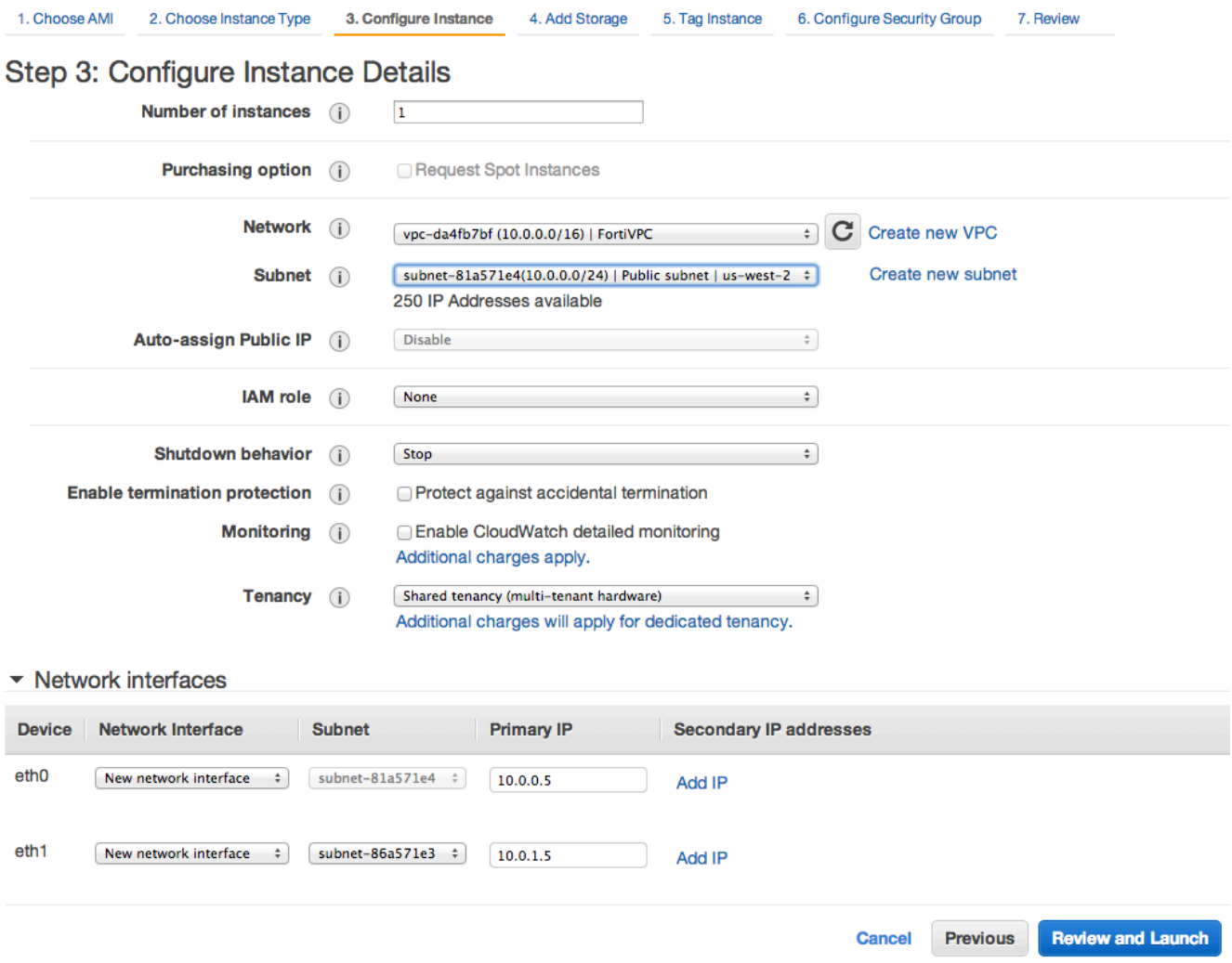
Step 3.2 – Instance type

Choose the instance type that matches the license. For this example we have a 1 vCPU license file.



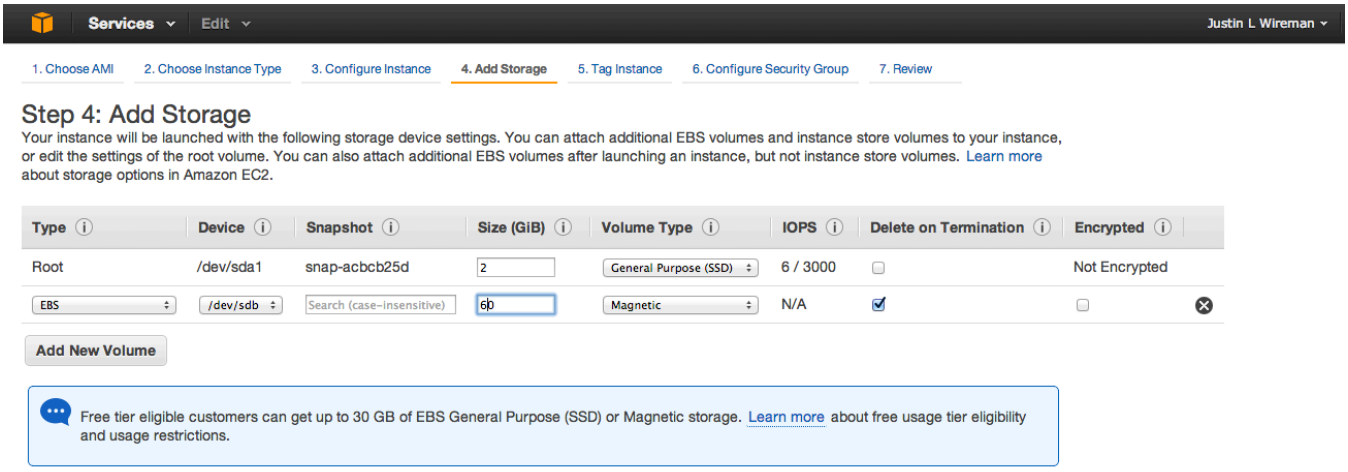
Step 3.3 – Instance Details

In this step you will choose the public subnet, assign IP addresses, and add the eth1 interface (private subnet).



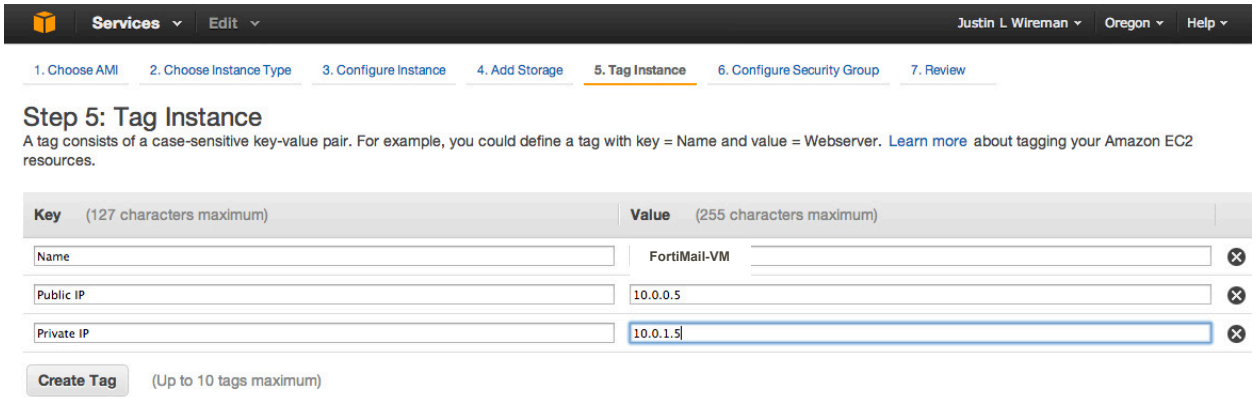
Step 3.4 – Instance Storage

If you are configuring this for demonstration purposes, you can change the highlighted storage size to create a larger disk size for logging / reporting.



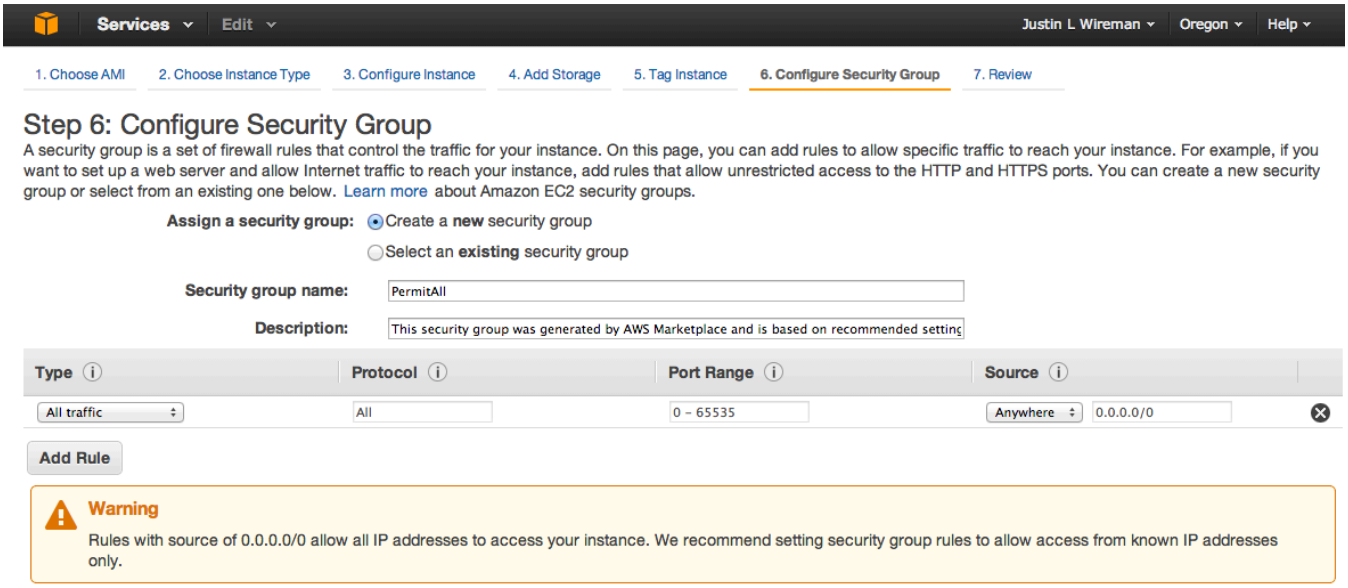
Step 3.5 – Instance Tags

It is valuable to create tags to quickly reference instance items in your AWS deployment. See the following example.



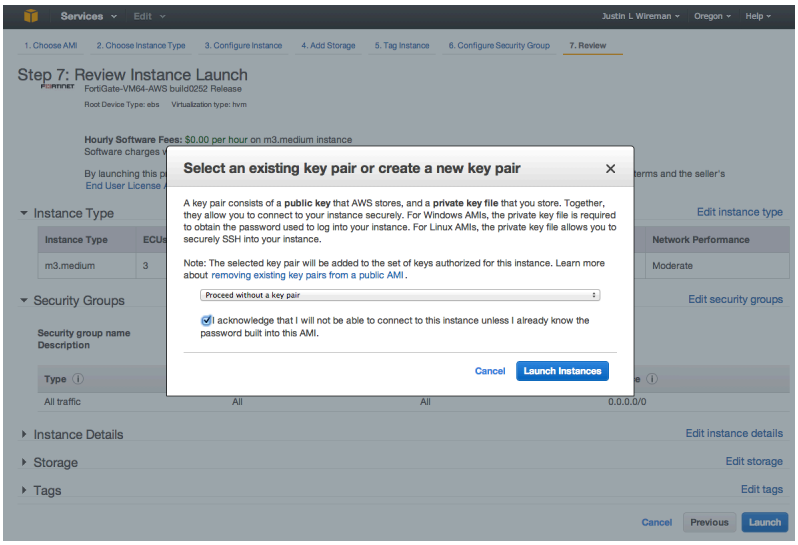
Step 3.6 – Security groups

Amazon by default has your VPC behind a basic firewall. Since we are going to be utilizing the FortiMail, let's create a Permit All security group and apply it to this instance.



Step 3.7 – Key Pair and Launch Instance

- Choose proceed without a keypair and use the default FortiMail username / password.
- Click Launch Instance to begin the provisioning.



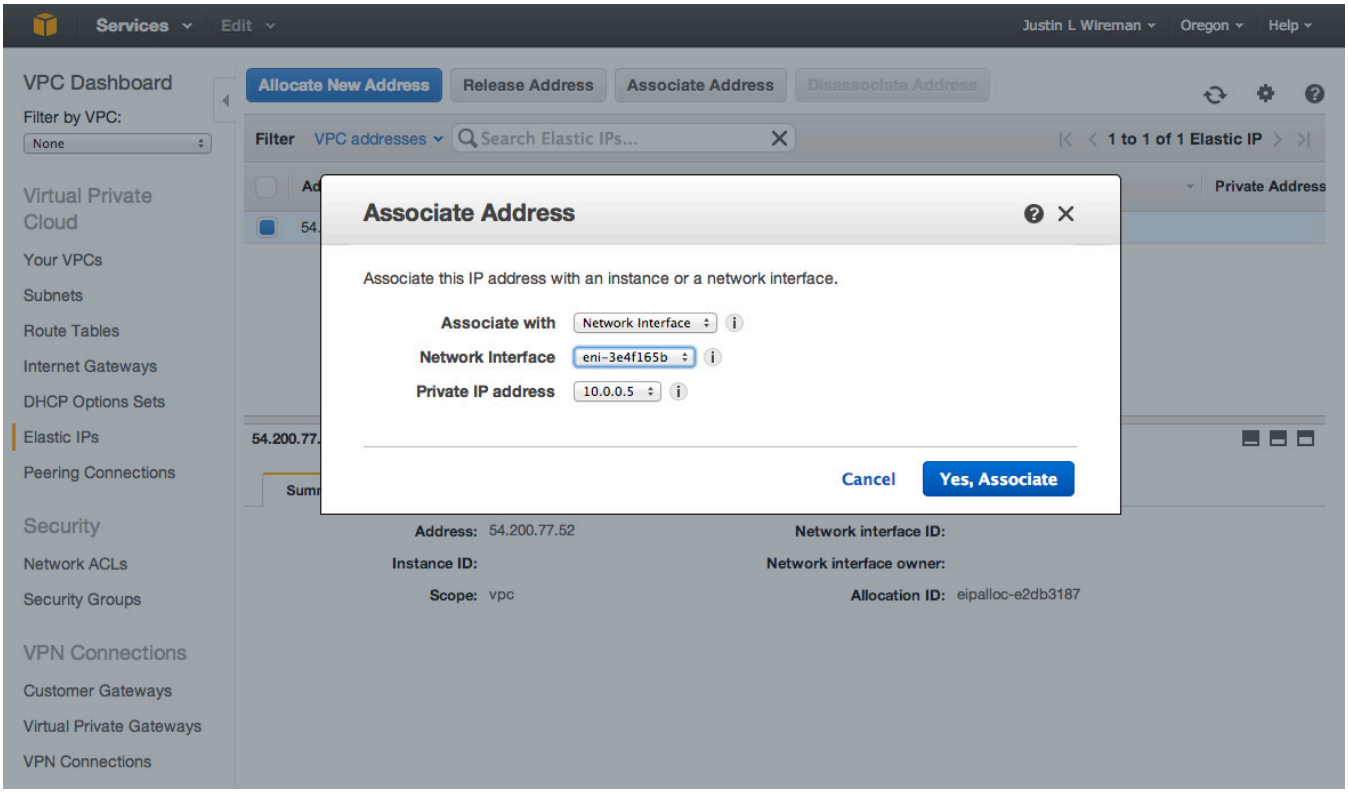
Network Configuration

In this section you will be locating items such as the Network interface ENI on the EC2 dashboard and making IP and routing updates on the VPC dashboard.

Step 4 – Configure AWS network settings

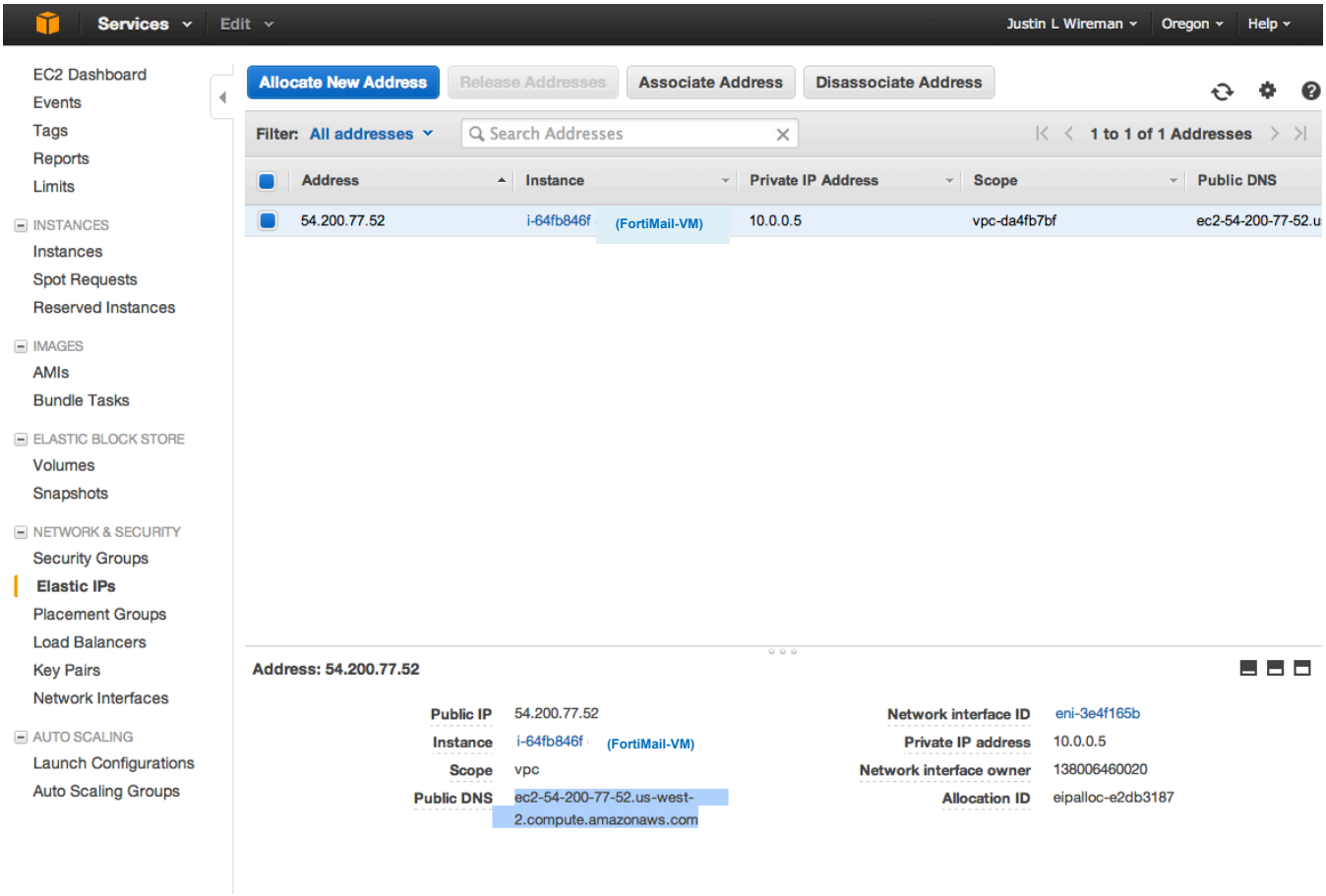
Step 4.1 - Associate a public "elastic" IP to the FE-VM public interface

- On the EC2 Dashboard under the Network interface menu.
  - Locate the public interface ENI.
    - See step 4.3 for a screenshot of this menu.
- On the VPC Dashboard under the Elastic IPs menu.
  - If the Public IP is associated with a default instance you will need to disassociate the Public IP before you can proceed.
  - Use the ENI of the public FortiMail interface as the object to associate the public IP.



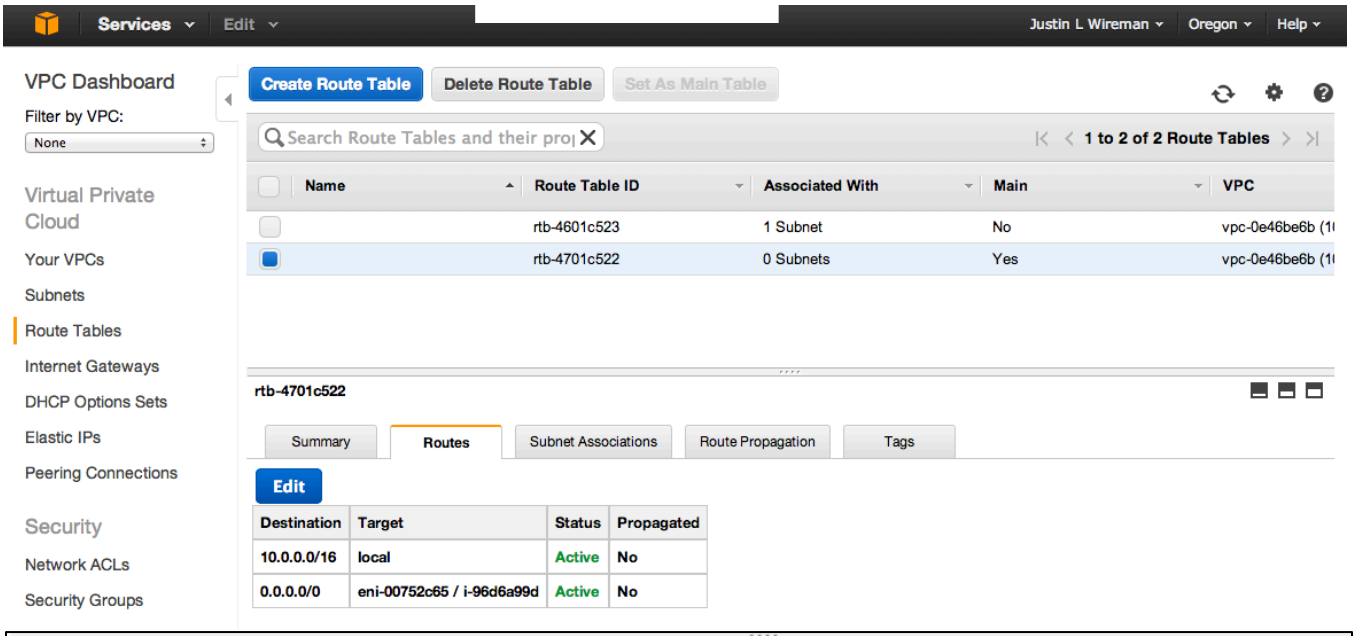
Step 4.2 – Confirm the assigned Public address

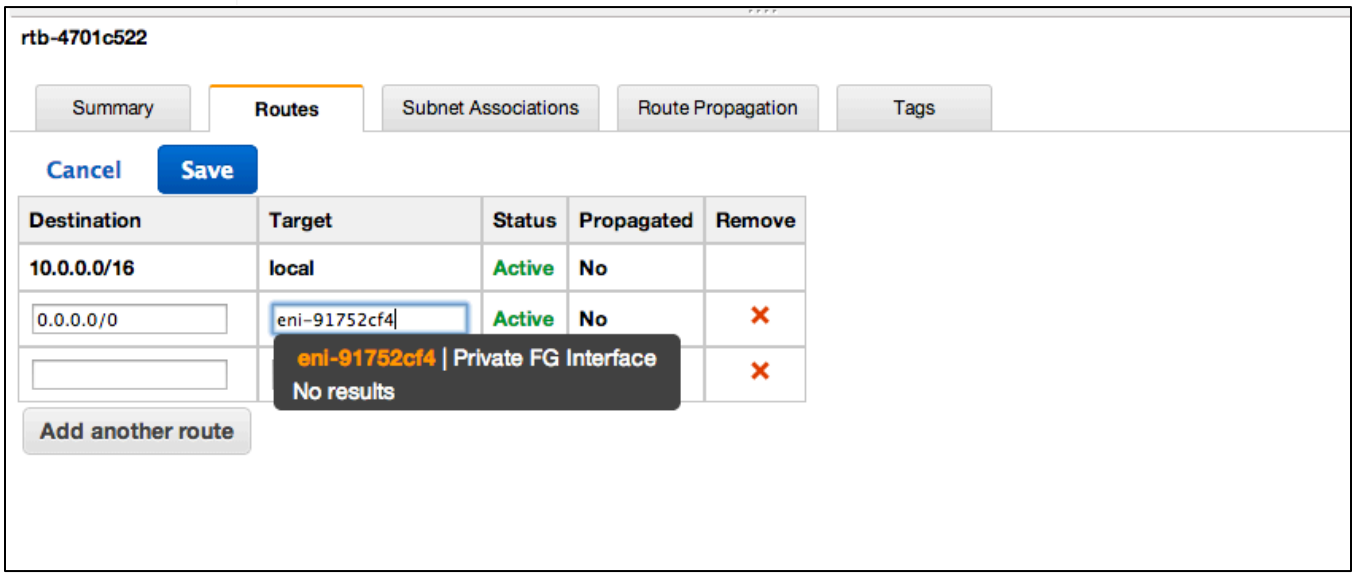
- Take note of the public IP address and DNS assigned. You will use these items in later steps.



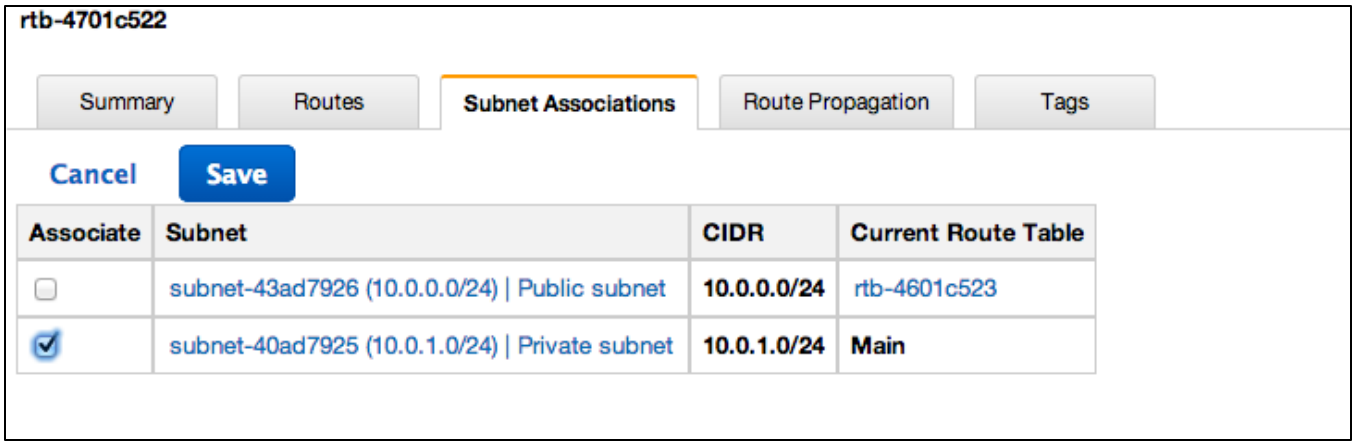
Step 4.3 – Setting up the default route for the private network.

- On the EC2 Dashboard under the Network interface menu.
  - Locate the network interface ID (ENI-) of the private network and Copy the ID.
- Change dashboards back to the VPC>Route Tables
  - Edit the default route (for the private subnet) to point to the FortiMail private network interface ID.



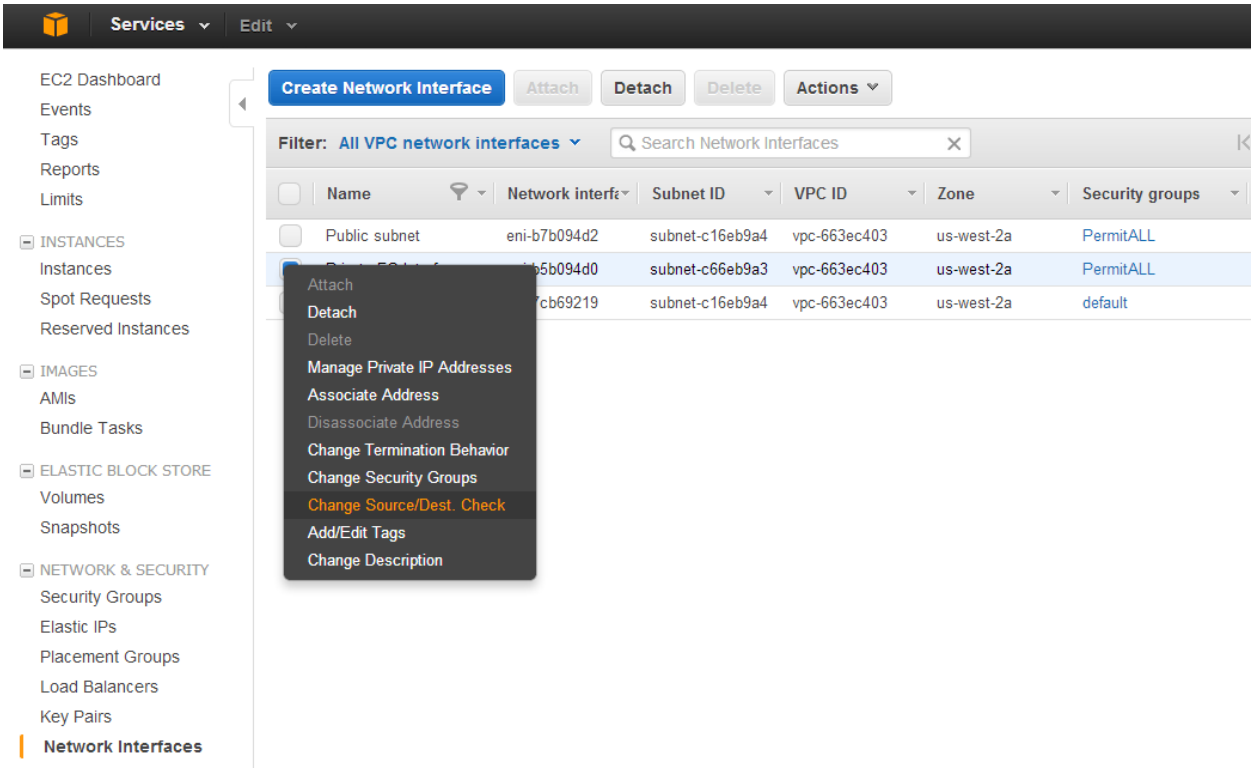


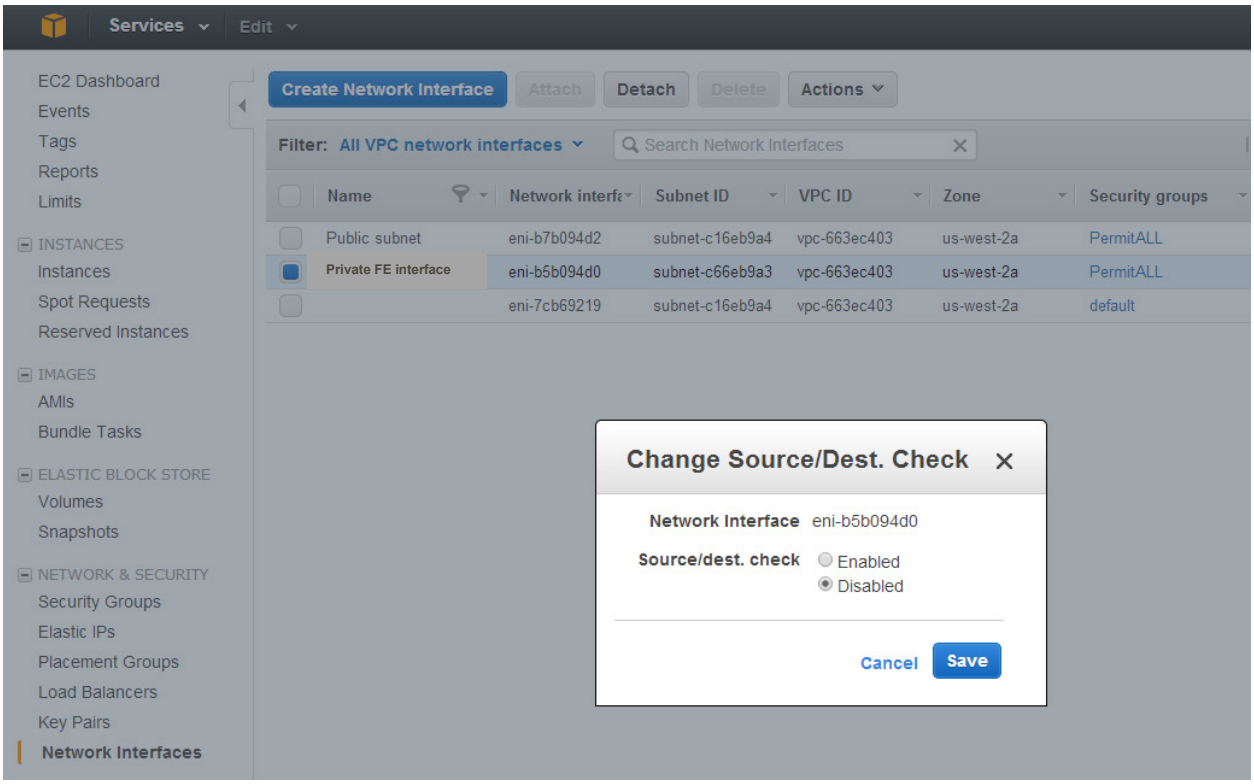
- Associate the private subnet to the private routing entry you have been editing in the previous steps.



Step 4.4 – Disable Source / Destination check on the Private FortiMail interface.

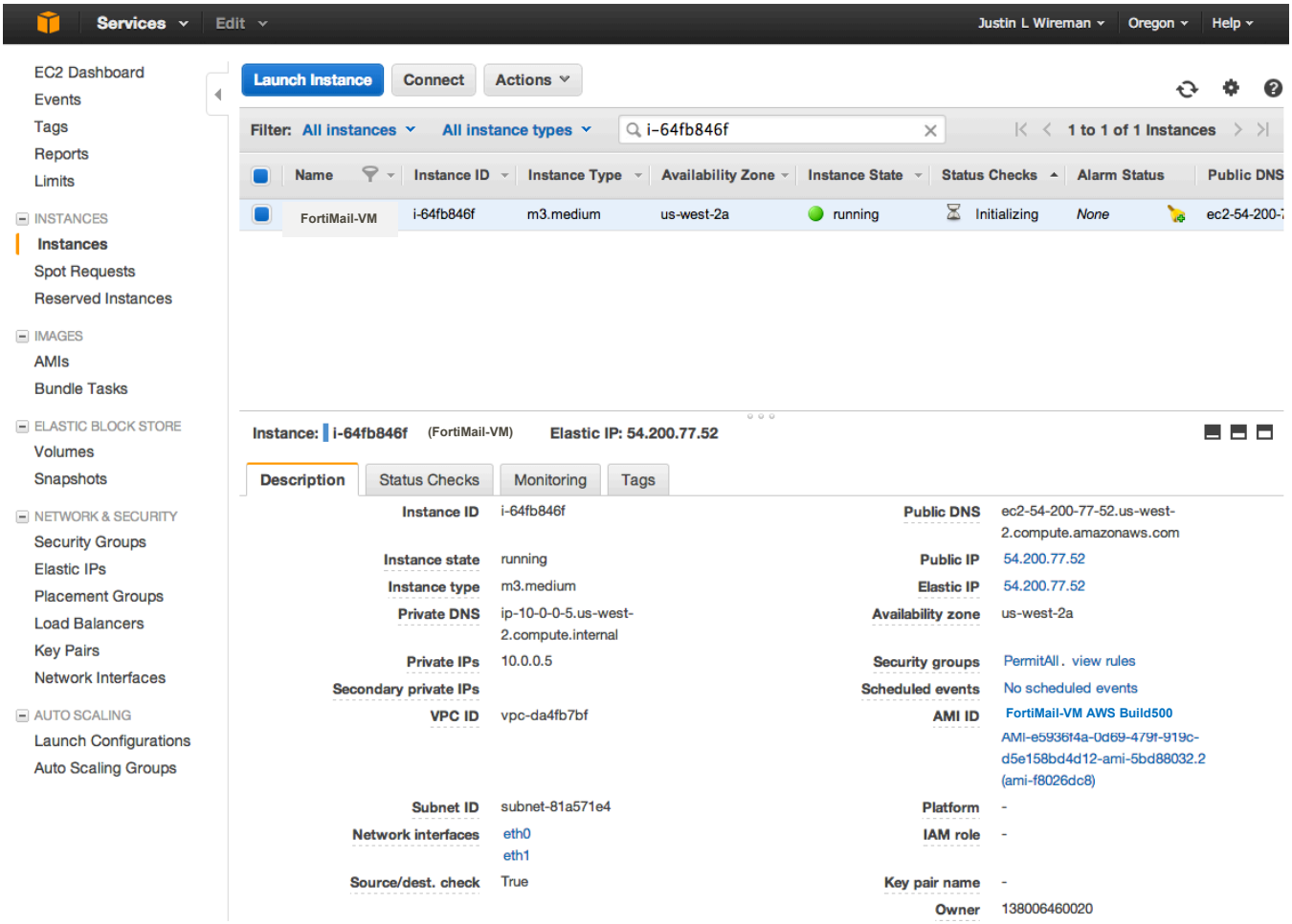
- On the EC2 Dashboard under the Network interface menu.
  - Right click and select Change Source/Dest Check
  - Select Disable and Save





Step 4.5 - Navigate to EC2 dash to review the Instance state

- Once confirming that the instance has finished provisioning and powering up check the following items.
    - Public IP/DNS assigned
    - Confirm the correct security group is assigned.


Services
Edit
Justin L Wireman
Oregon
Help
EC2 Dashboard
Events
Tags
Reports
Limits
INSTANCES
Instances
Spot Requests
Reserved Instances
IMAGES
AMIs
Bundle Tasks
ELASTIC BLOCK STORE
Volumes
Snapshots
NETWORK & SECURITY
Security Groups
Elastic IPs
Placement Groups
Load Balancers
Key Pairs
Network Interfaces
AUTO SCALING
Launch Configurations
Auto Scaling Groups
Launch Instance
Connect
Actions
Filter: All instances
All instance types
i-64fb846f
1 to 1 of 1 Instances
Name
Instance ID
Instance Type
Availability Zone
Instance State
Status Checks
Alarm Status
Public DNS
FortiMail-VM
i-64fb846f
m3.medium
us-west-2a
running
Initializing
None
Instance: i-64fb846f (FortiMail-VM)
Elastic IP: 54.200.77.52
Description
Status Checks
Monitoring
Tags
Instance ID
i-64fb846f
Instance state
running
Instance type
m3.medium
Private DNS
ip-10-0-0-5.us-west-2.compute.internal
Private IPs
10.0.0.5
Secondary private IPs
VPC ID
vpc-da4fb7bf
Subnet ID
subnet-81a571e4
Network interfaces
eth0
eth1
Source/dest. check
True
Public DNS
ec2-54-200-77-52.us-west-2.compute.amazonaws.com
Public IP
54.200.77.52
Elastic IP
54.200.77.52
Availability zone
us-west-2a
Security groups
PermitAll. view rules
Scheduled events
No scheduled events
AMI ID
FortiMail-VM AWS Build500
AMI-e5936f4a-0d69-479f-919c-d5e158bd4d12-ami-5bd88032.2 (ami-f8026dc8)
Platform
-
IAM role
-
Key pair name
-
Owner
138006460020

Step 4.6 - Access the Virtual FortiMail

- Open a HTTPS session to the public IP or DNS entry provided and login with the default username / password (default username is admin and default password is the AWS instance ID). For example: https://54.200.77.52/admin (make sure to include /admin)

Step 4.7 – SSH to the FortiMail unit

- SSH to the device using the public IP address or the DNS hostname
- Issue the following commands to test access

```
FortiMail-VM64-AWS# execute ping 8.8.8.8
```

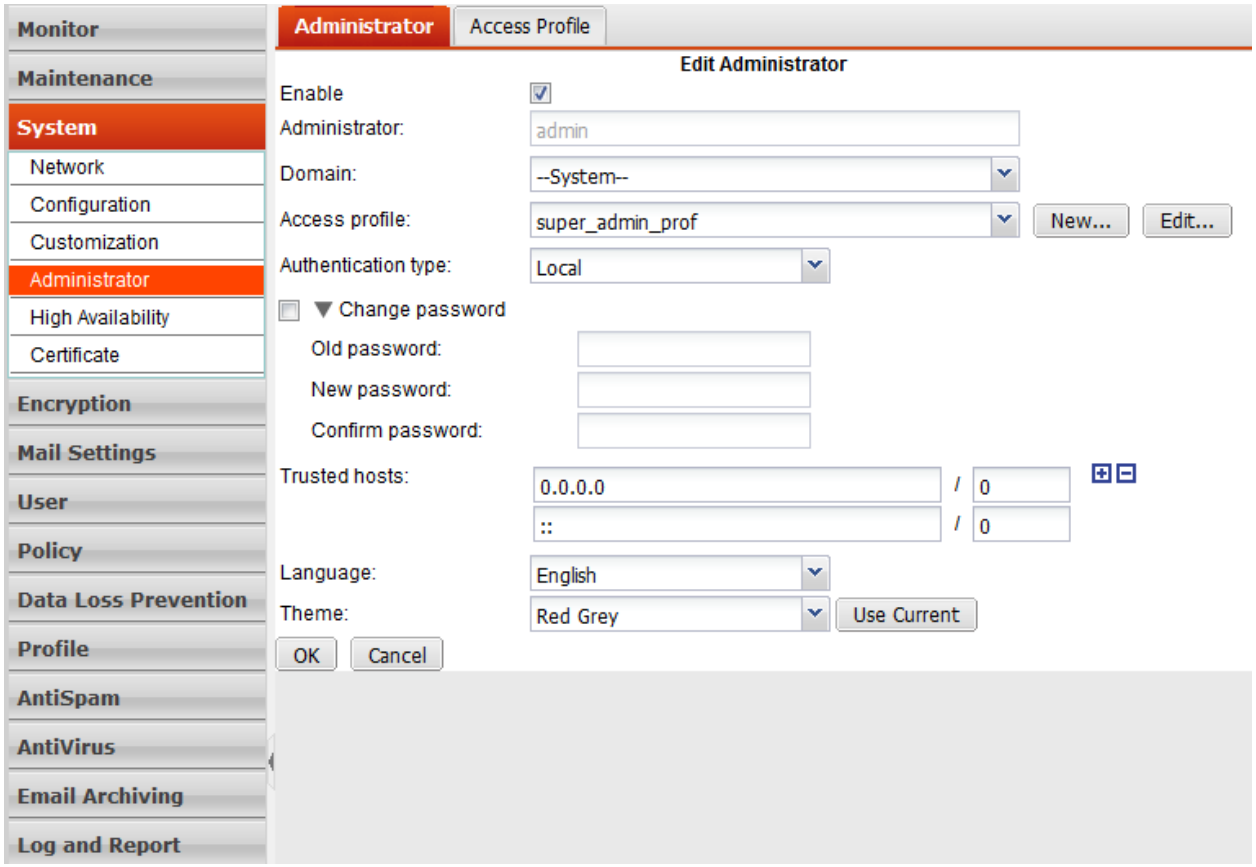
FortiMail Configuration

After you log on to FortiMail, you can start to configure the system. For details, see the FortiMail Administration Guide on https://docs.fortinet.com.

Step 5.1 - Update admin password

Update the FortiMail administrator password as there are many bots that attempt to log in to newly provisioned devices on AWS subnets.

To change the admin password, go to **System > Administrator**. Edit the admin user and set up the password. By default, the admin user does not have a password.



Step 5.2 - Install the license

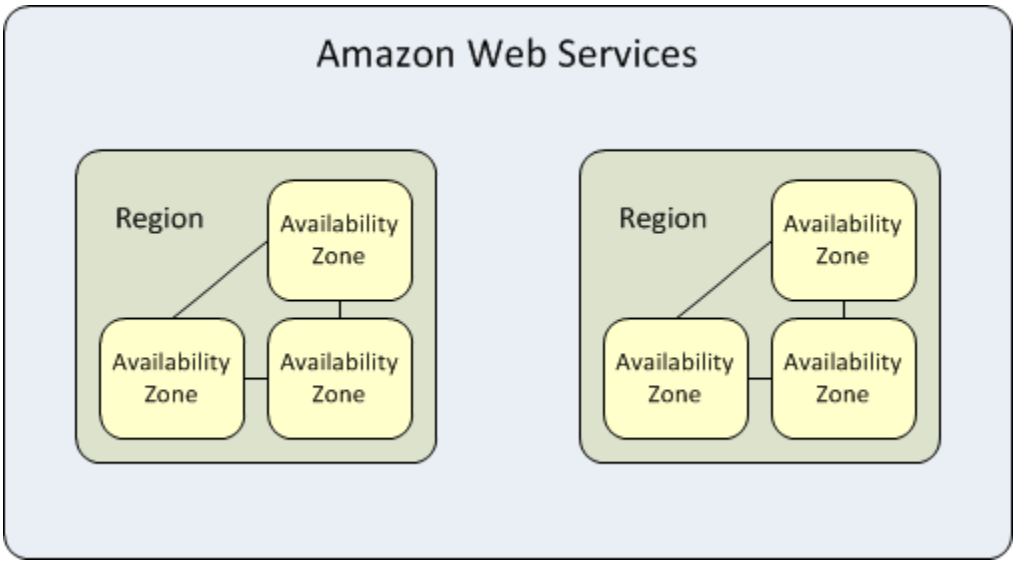
In the **License Information** widget on the FortiMail VM web-based manager, click the **Upload License** link to the right of **VM License**, then upload the license.

Appendix

Regions and Availability Zones

Region and Availability Zone Concepts

Each region is completely independent. Each Availability Zone is isolated, but the Availability Zones in a region are connected through low-latency links. The following diagram illustrates the relationship between regions and Availability Zones.



You can list the Availability Zones that are available to your account. For more information, see Describing Your Regions and Availability Zones. When you launch an instance, you can select an Availability Zone or let us choose one for you. If you distribute your instances across multiple Availability Zones and one instance fails, you can design your application so that an instance in another Availability Zone can handle requests.

Amazon EC2 resources are either global, tied to a region, or tied to an Availability Zone. For more information, see AWS documentation for the complete article.

Amazon EC2 Key Pairs

Amazon EC2 uses public–key cryptography to encrypt and decrypt login information. Public–key cryptography uses a public key to encrypt a piece of data, such as a password, then the recipient uses the private key to decrypt the data. The public and private keys are known as a ***key pair***.

To log in to your instance, you must create a key pair, specify the name of the key pair when you launch the instance, and provide the private key when you connect to the instance. Linux/Unix instances have no password, and you use a key pair to log in using SSH. With Windows instances, you use a key pair to obtain the administrator password and then log in using RDP.

Creating a Key Pair

You can use Amazon EC2 to create your key pair. For more information, see Creating Your Key Pair Using Amazon EC2. Alternatively, you could use a third-party tool and then import the public key to Amazon EC2. For more information, see Importing Your Own Key Pair to Amazon EC2.

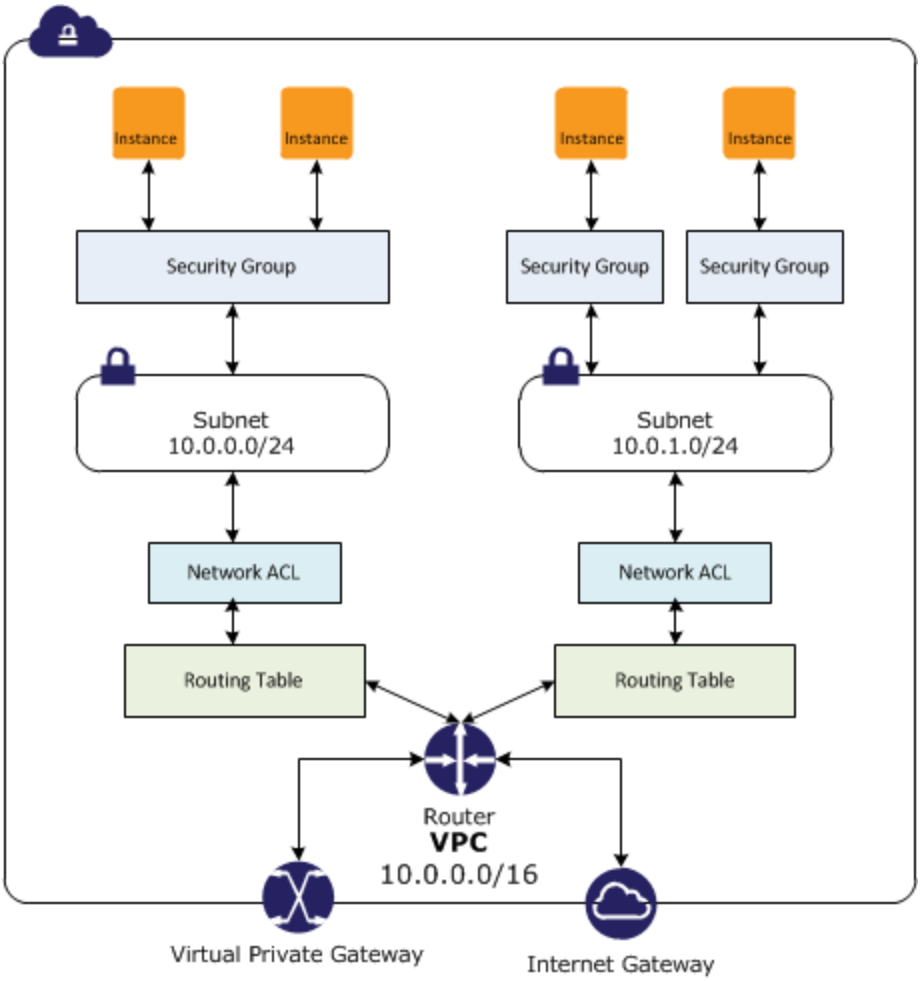
Each key pair requires a name. Be sure to choose a name that is easy to remember. Amazon EC2 associates the public key with the name that you specify as the key name. Amazon EC2 stores the public key only, and you store the private key. Anyone who possesses your private key can decrypt your login information, so it's important that you store your private keys in a secure place.

The keys that Amazon EC2 uses are 1024-bit SSH-2 RSA keys. You can have up to five thousand key pairs per region.

Launching and Connecting to Your Instance

When you launch an instance, you should specify the name of the key pair you plan to use to connect to the instance. If you don't specify the name of an existing key pair when you launch an instance, you won't be able to connect to the instance. When you connect to the instance, you must specify the private key that corresponds to the key pair you specified when you launched the instance. Amazon EC2 doesn't keep a copy of your private key; therefore, if you lose your private key, there is no way to recover it. If you lose the private key for an instance store-backed instance, you can't access the instance; you should terminate the instance and launch another instance using a new key pair. If you lose the private key for an EBS-backed instance, you can regain access to your instance. For more information, see Connecting to Your Instance if You Lose Your Private Key.

Detailed VPC Diagram



Additional info and links

http://aws.amazon.com/documentation/vpc/

http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Introduction.html