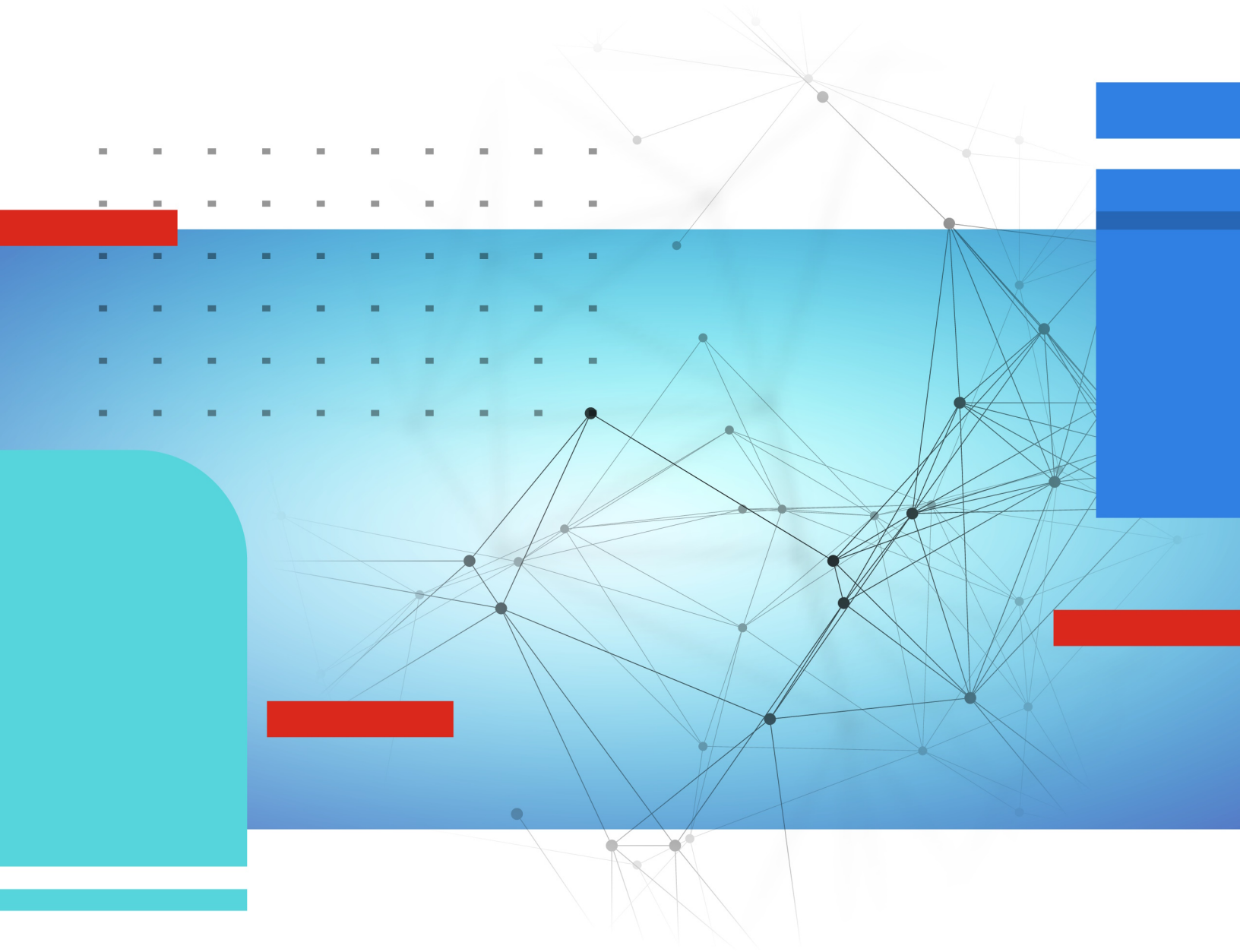
AWS Deployment Guide

FortiMail 7.6.0



FORTINET DOCUMENT LIBRARY
https://docs.fortinet.com

FORTINET VIDEO LIBRARY
https://video.fortinet.com

FORTINET BLOG
https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT
https://support.fortinet.com

FORTINET TRAINING & CERTIFICATION PROGRAM
https://www.fortinet.com/training-certification

FORTINET TRAINING INSTITUTE
https://training.fortinet.com

FORTIGUARD LABS
https://www.fortiguard.com

END USER LICENSE AGREEMENT
https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK
Email: techdoc@fortinet.com

October 18, 2024
FortiMail 7.6.0 AWS Deployment Guide
06-760-000000-20241018

TABLE OF CONTENTS

Change Log

Date	Change Description
2024-10-18	Initial release of FortiMail 7.6.0 AWS Deployment Guide.

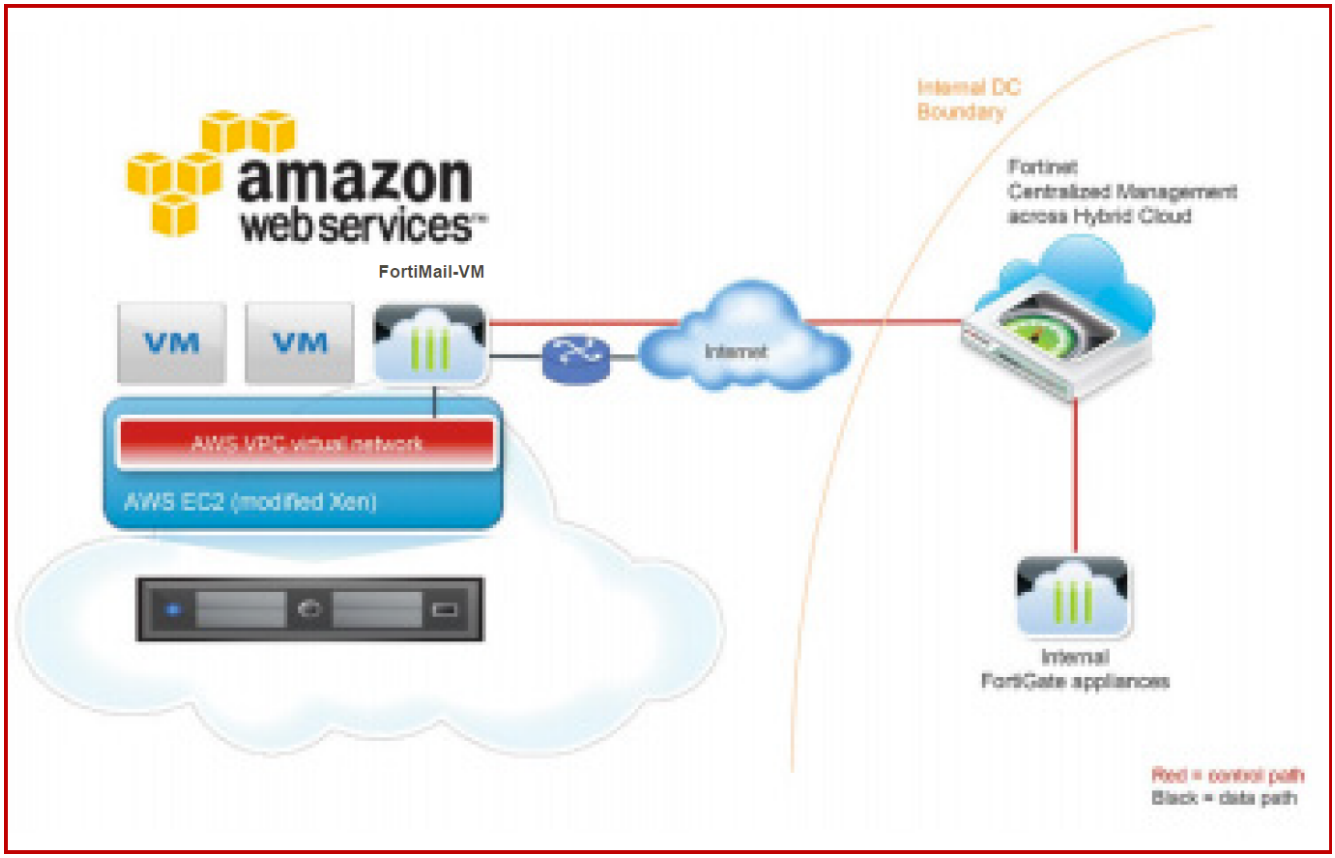
Overview

This document is designed to be a quick start walk-though in setting up a virtual FortiMail device utilizing Amazon Web Services (AWS).

Amazon Virtual Private Cloud (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?

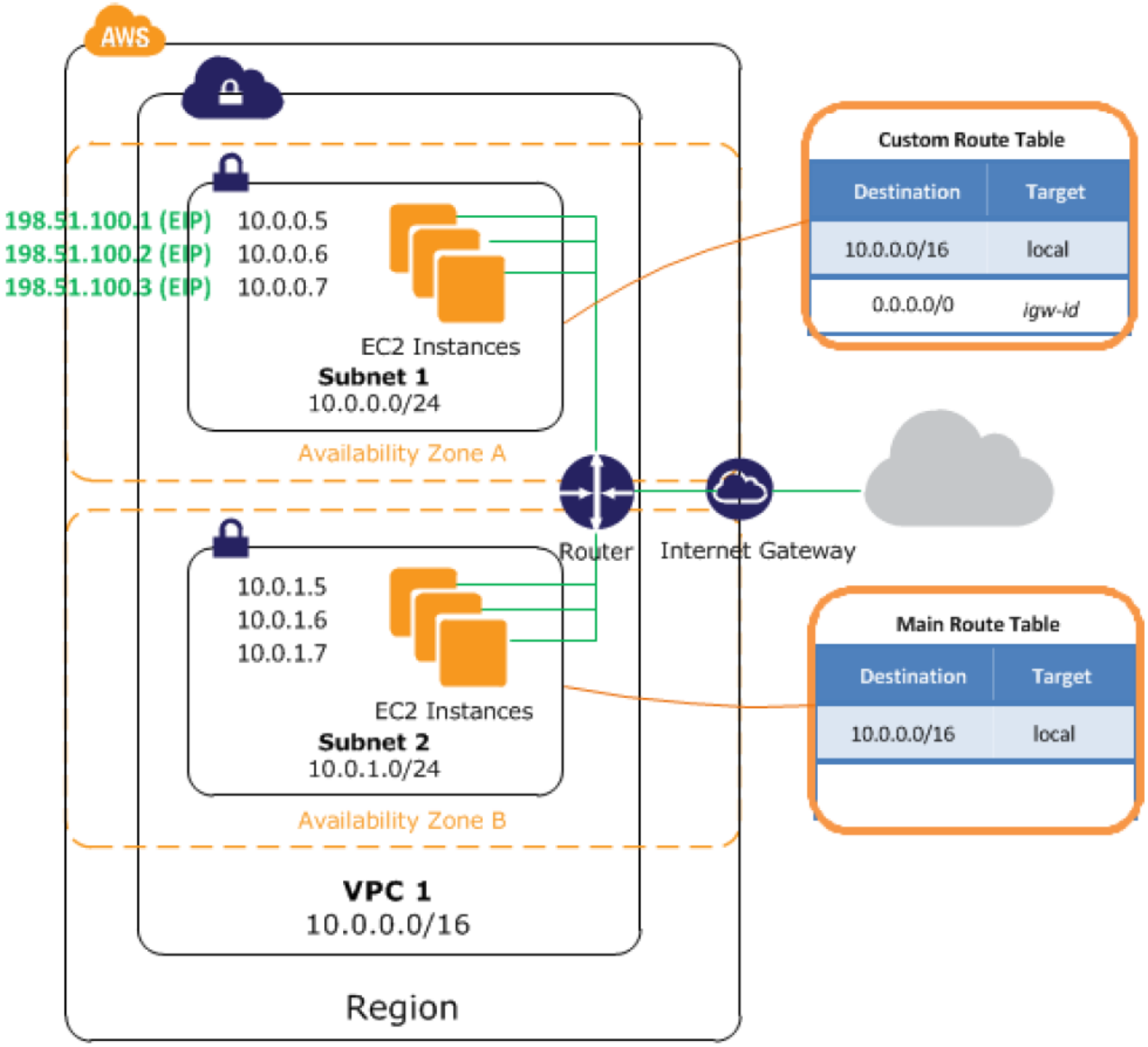
Instances without EIPs can access the Internet in one of two ways:

1. 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.
2. 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

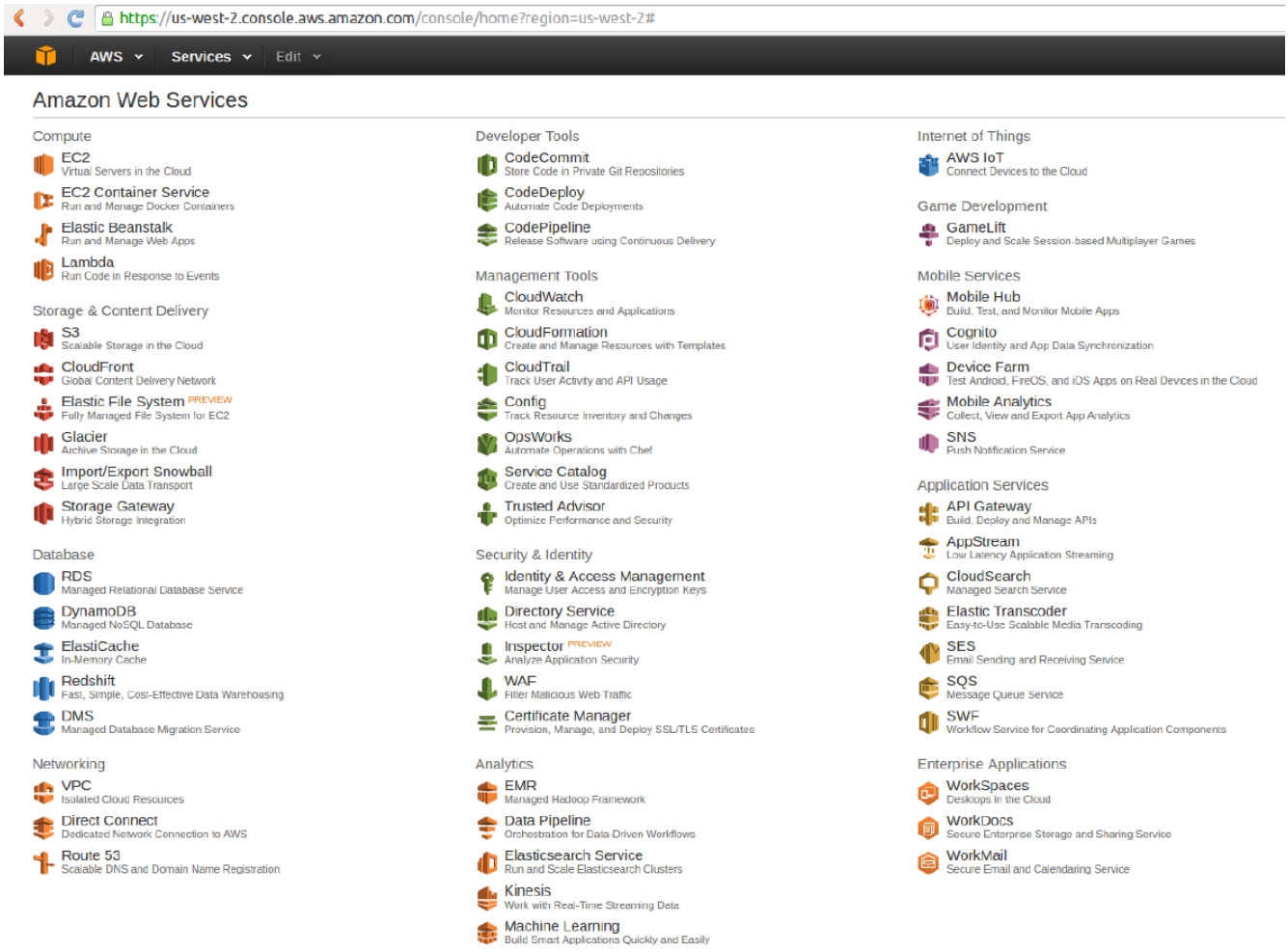


Warning: AWS blocks outbound traffic on port 25 (SMTP) of all EC2 instances by default. For information about how to remove the restriction, see:
https://repost.aws/knowledge-center/ec2-port-25-throttle

Basic AWS Network Setup

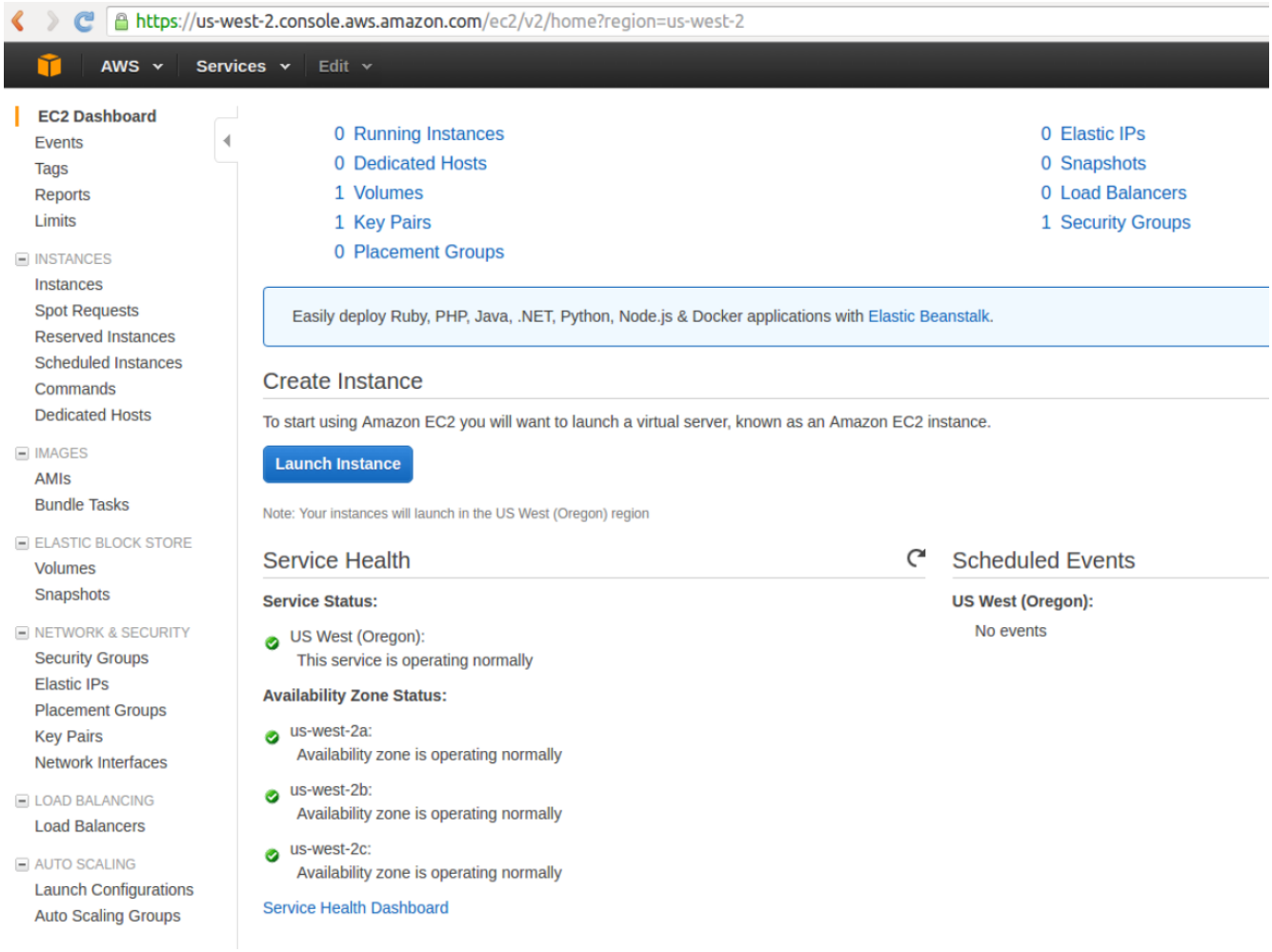
Setting up your AWS account

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.



Creating a Virtual Private Cloud (VPC)

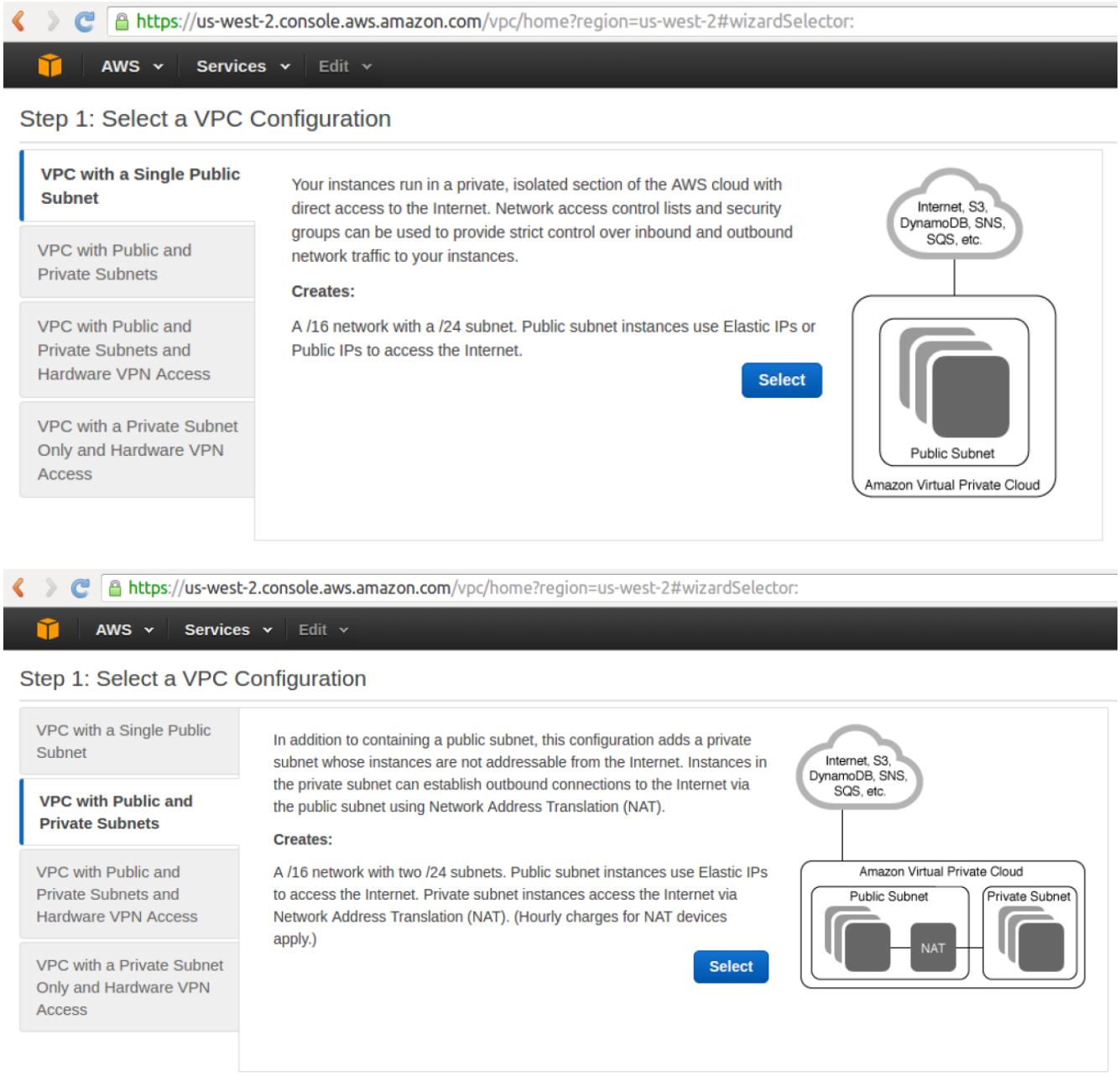
To allow VM instances access to more than one interface you need to create a VPC (virtual private cloud). You need to change dashboards to VPC and for our purpose start the VPC wizard.



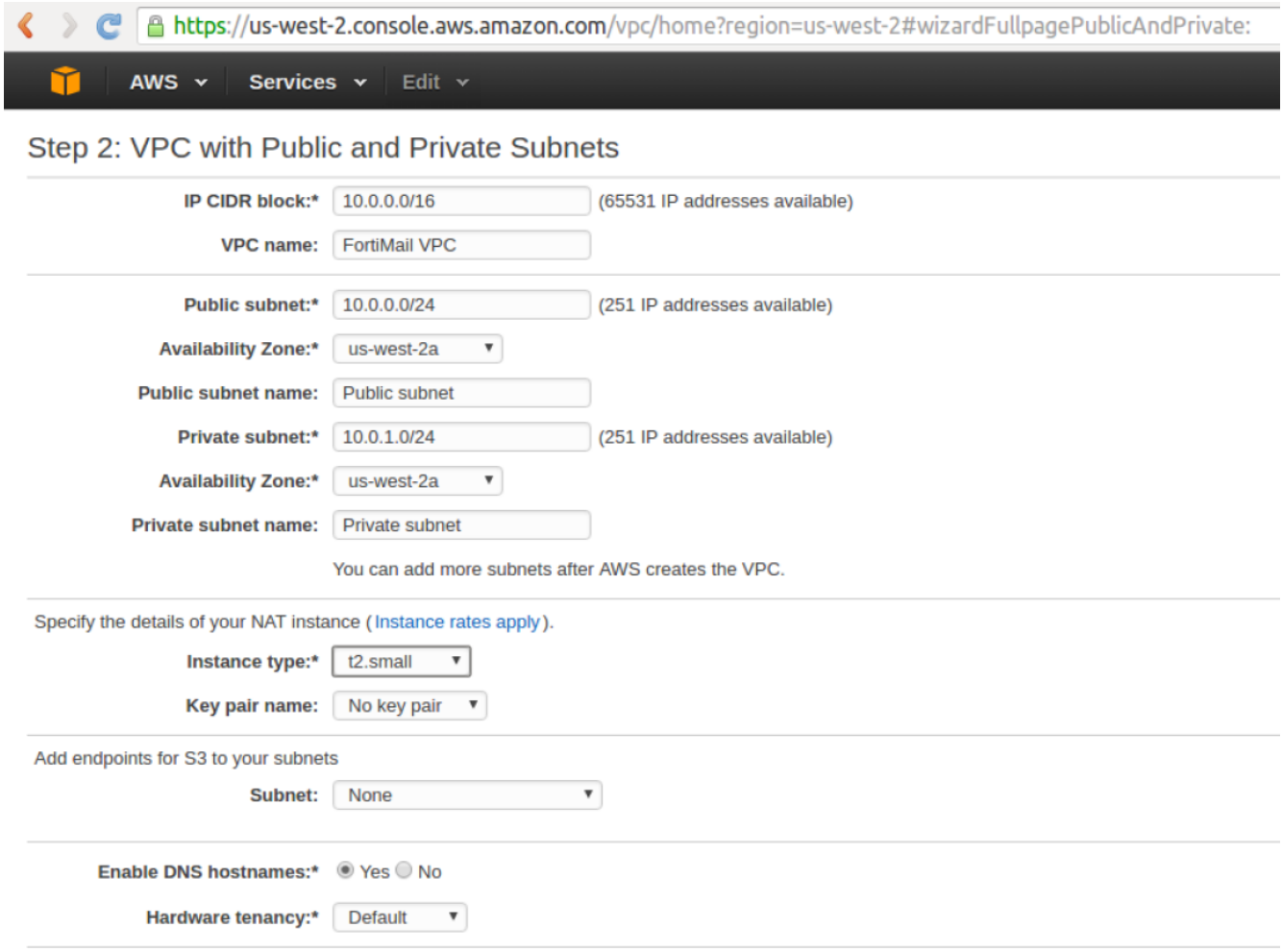
It is important to note that like most multi-tenant environments AWS reserves the first 5 IP address of each network that is created for its own router/firewall and DHCP/DNS servers.

VPC Wizard

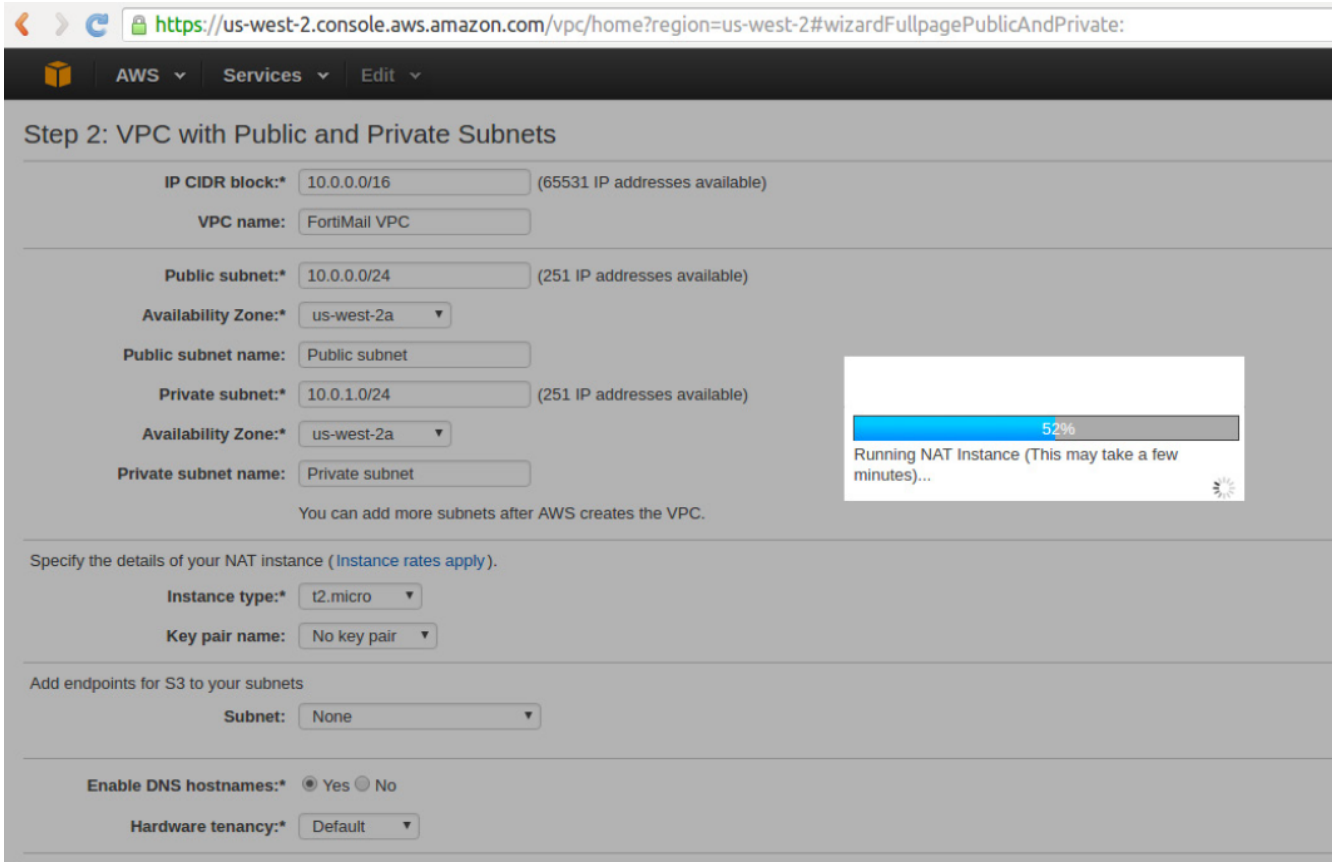
This next section is a visual walk-through of the VPC wizard. Select the Public and Private subnet option.



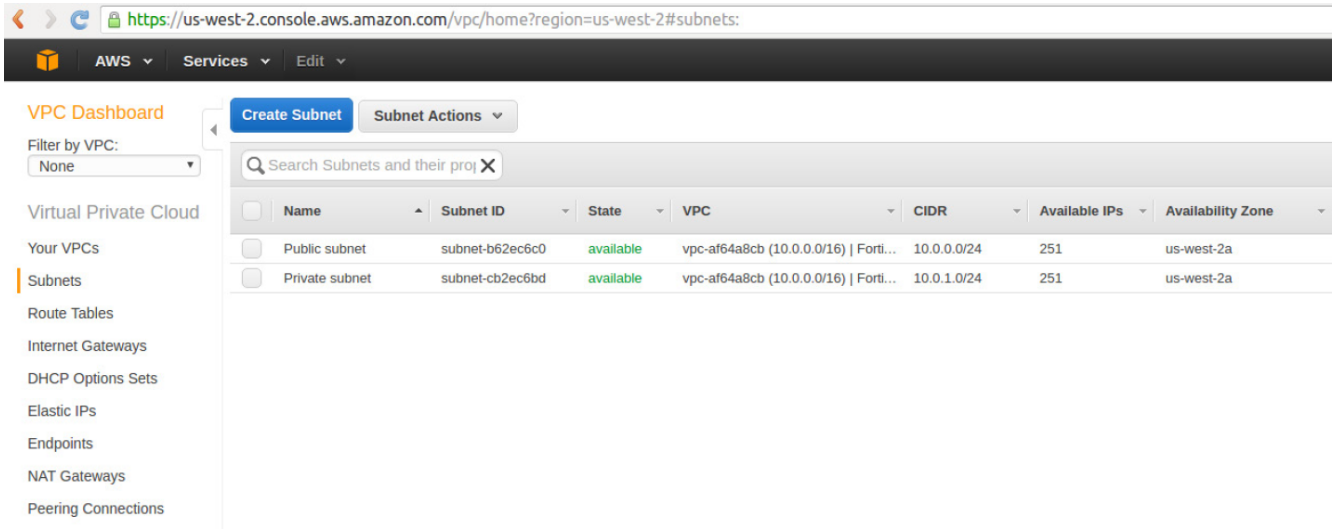
One item to double check on step 2 of the VPC wizard is to make sure that both subnets are in the **same availability zone**. Please see the Appendix on page 26 for more information on availability zones.



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



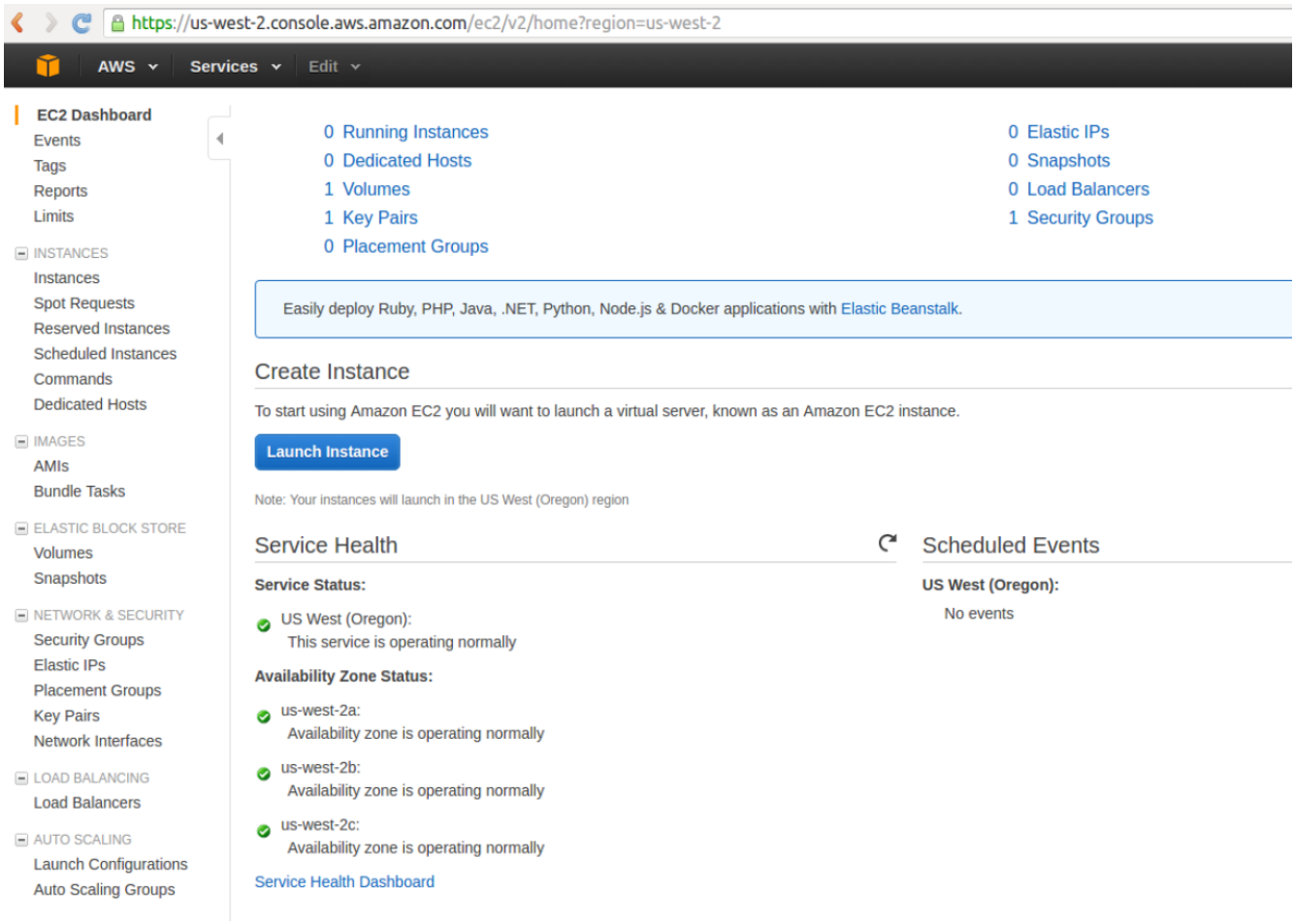
When the VPC setup has been completed you can review subnet and routing information on the VPC Dashboard.



FortiMail Provisioning

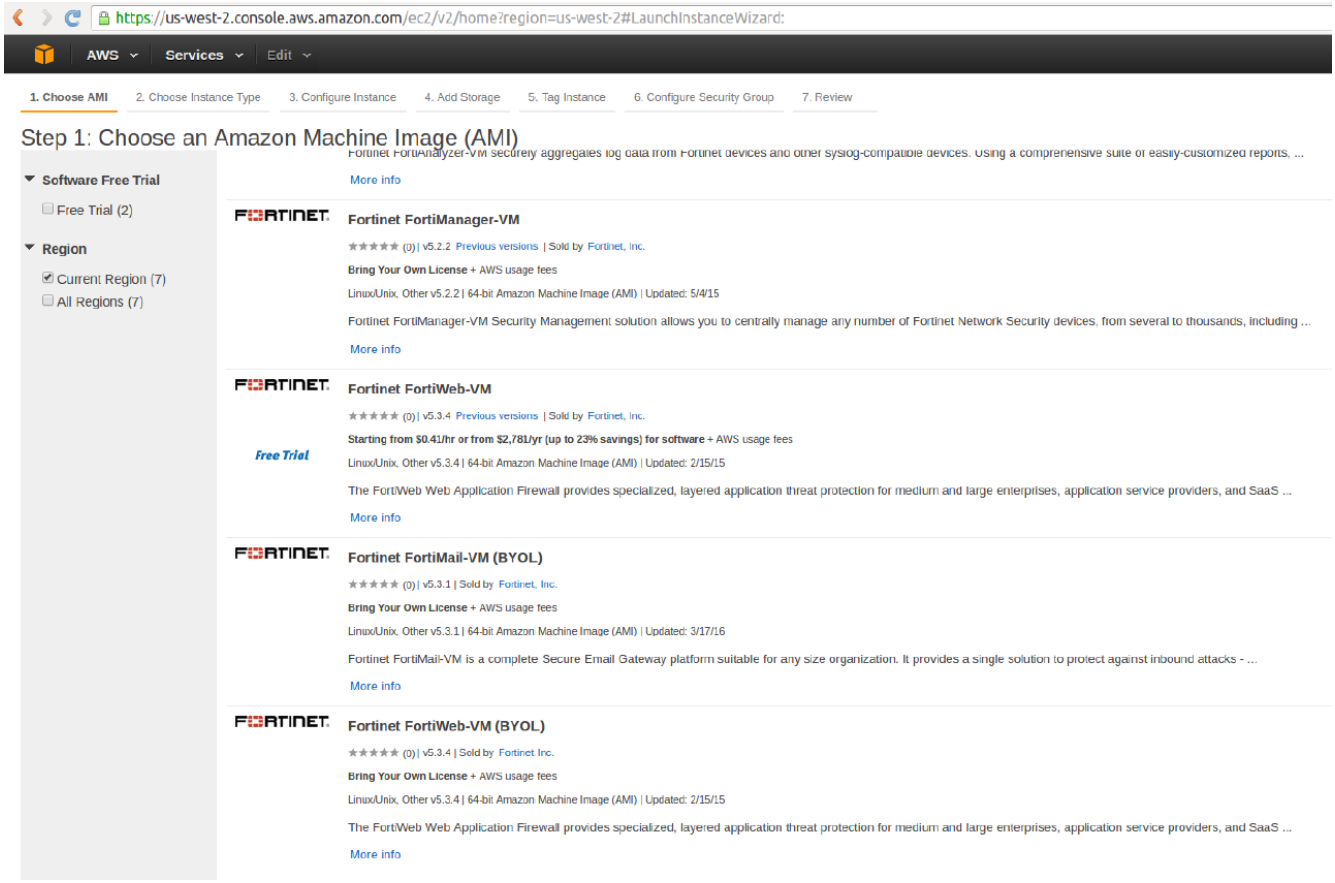
EC2 launching virtual machines

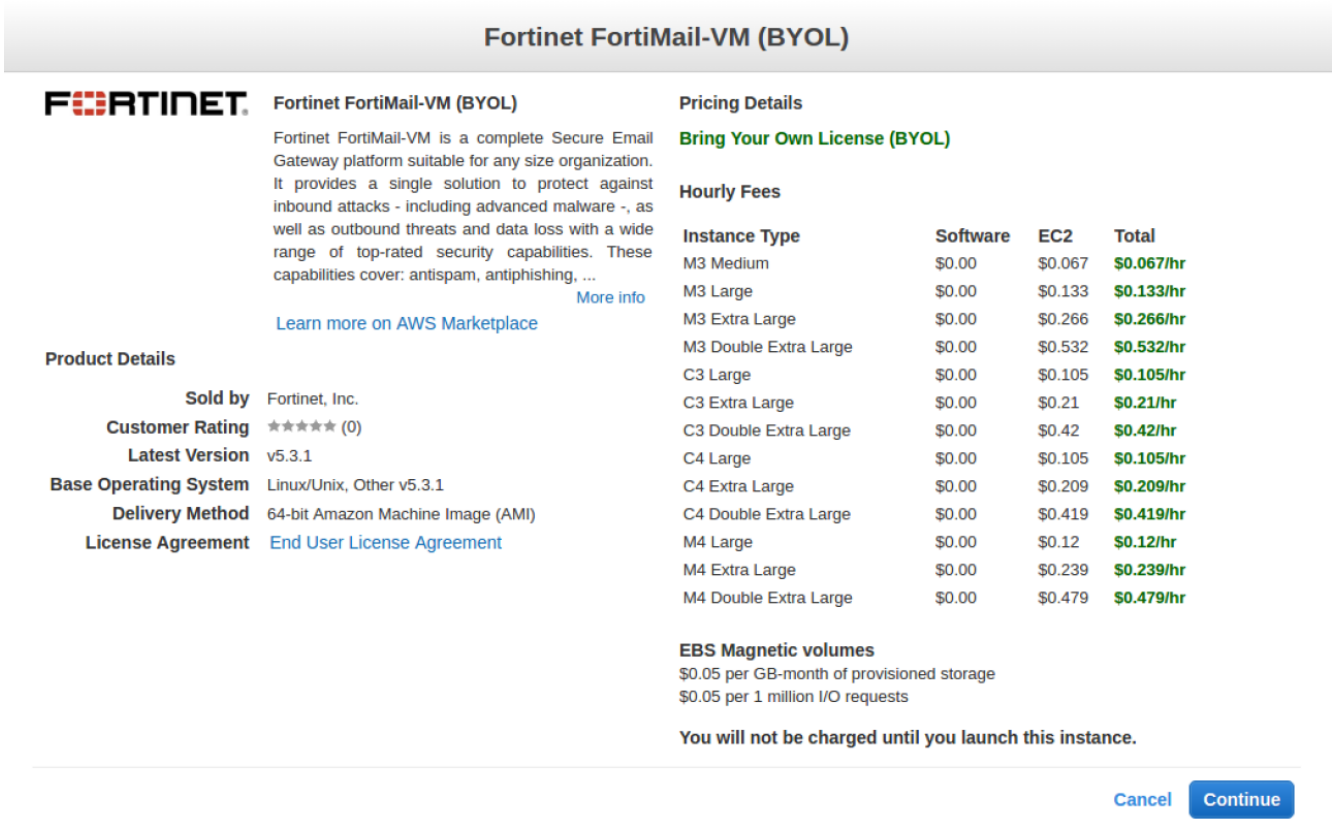
Change dashboards to the EC2 dashboard. To save time, it is normally faster to get the VM provisioning started while setting up the network. Click Launch Instance on this screen.



Choosing an AMI

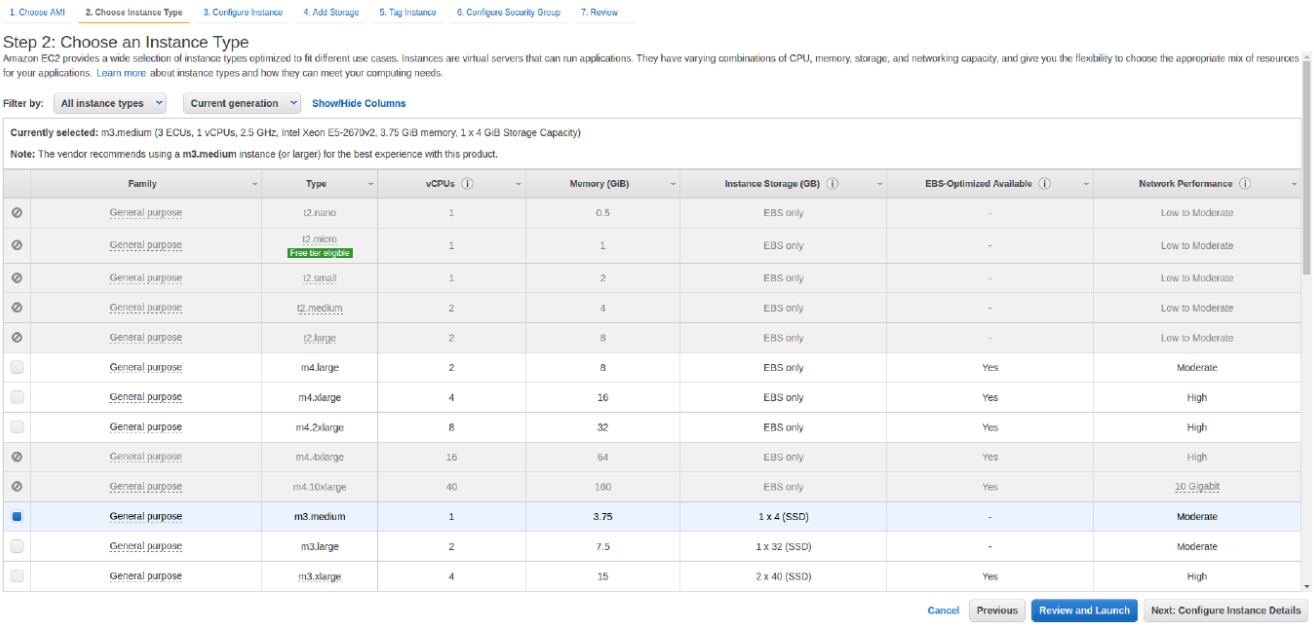
For this guide, the Bring Your Own License (BYOL) version of the FortiMail VM is used.


https://us-west-2.console.aws.amazon.com/ec2/v2/home?region=us-west-2#LaunchInstanceWizard:
AWS
Services
Edit
1. Choose AMI
2. Choose Instance Type
3. Configure Instance
4. Add Storage
5. Tag Instance
6. Configure Security Group
7. Review
Step 1: Choose an Amazon Machine Image (AMI)
Software Free Trial
Free Trial (2)
Region
Current Region (7)
All Regions (7)
More info
Fortinet FortiManager-VM
(0) | v5.2.2 Previous versions | Sold by Fortinet, Inc.
Bring Your Own License + AWS usage fees
Linux/Unix, Other v5.2.2 | 64-bit Amazon Machine Image (AMI) | Updated: 5/4/15
Fortinet FortiManager-VM Security Management solution allows you to centrally manage any number of Fortinet Network Security devices, from several to thousands, including ...
More info
Fortinet FortiWeb-VM
(0) | v5.3.4 Previous versions | Sold by Fortinet, Inc.
Free Trial
Starting from $0.41/hr or from $2,781/yr (up to 23% savings) for software + AWS usage fees
Linux/Unix, Other v5.3.4 | 64-bit Amazon Machine Image (AMI) | Updated: 2/15/15
The FortiWeb Web Application Firewall provides specialized, layered application threat protection for medium and large enterprises, application service providers, and SaaS ...
More info
Fortinet FortiMail-VM (BYOL)
(0) | v5.3.1 | Sold by Fortinet, Inc.
Bring Your Own License + AWS usage fees
Linux/Unix, Other v5.3.1 | 64-bit Amazon Machine Image (AMI) | Updated: 3/17/16
Fortinet FortiMail-VM is a complete Secure Email Gateway platform suitable for any size organization. It provides a single solution to protect against inbound attacks - ...
More info
Fortinet FortiWeb-VM (BYOL)
(0) | v5.3.4 | Sold by Fortinet Inc.
Bring Your Own License + AWS usage fees
Linux/Unix, Other v5.3.4 | 64-bit Amazon Machine Image (AMI) | Updated: 2/15/15
The FortiWeb Web Application Firewall provides specialized, layered application threat protection for medium and large enterprises, application service providers, and SaaS ...
More info



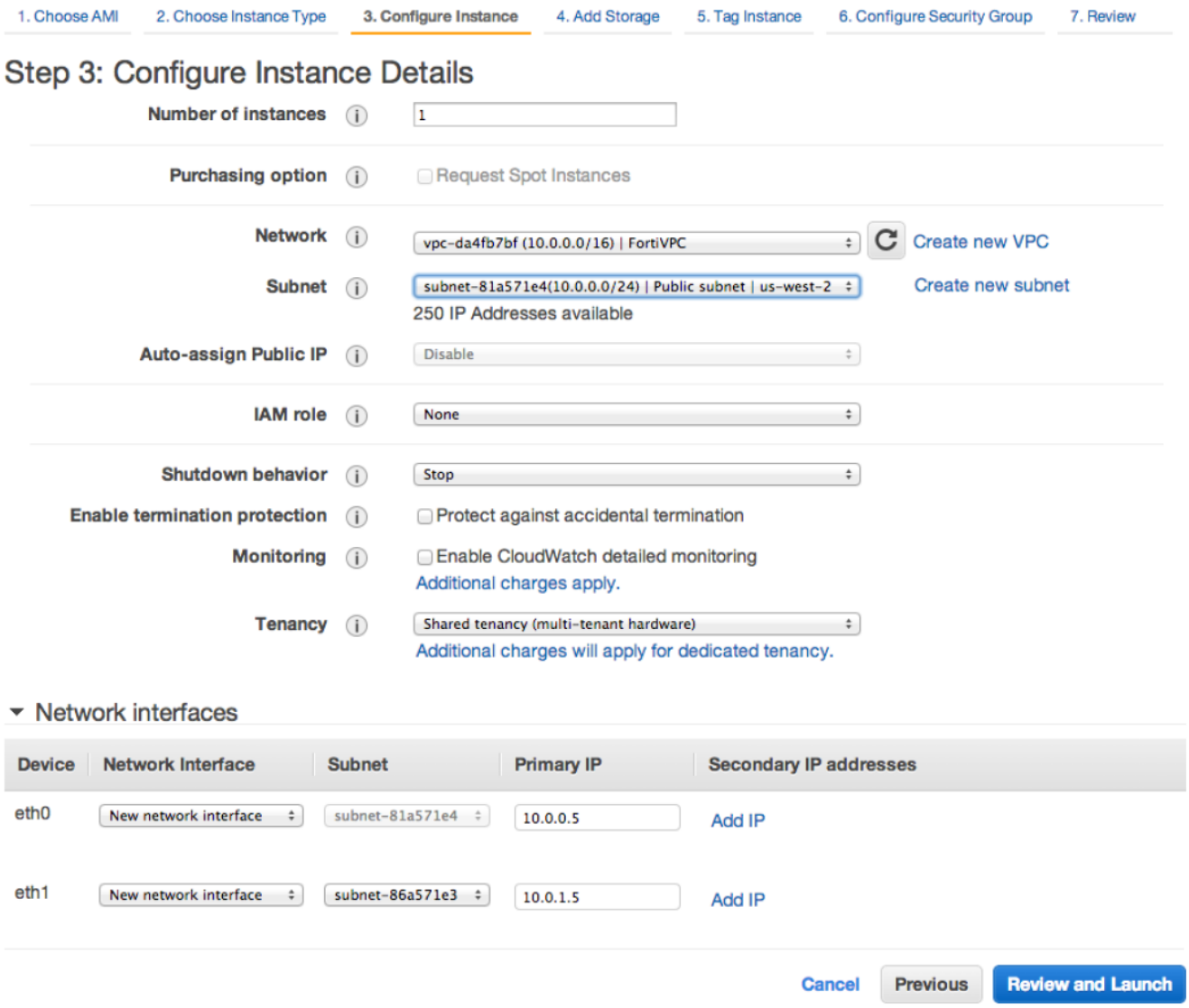
Instance type

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



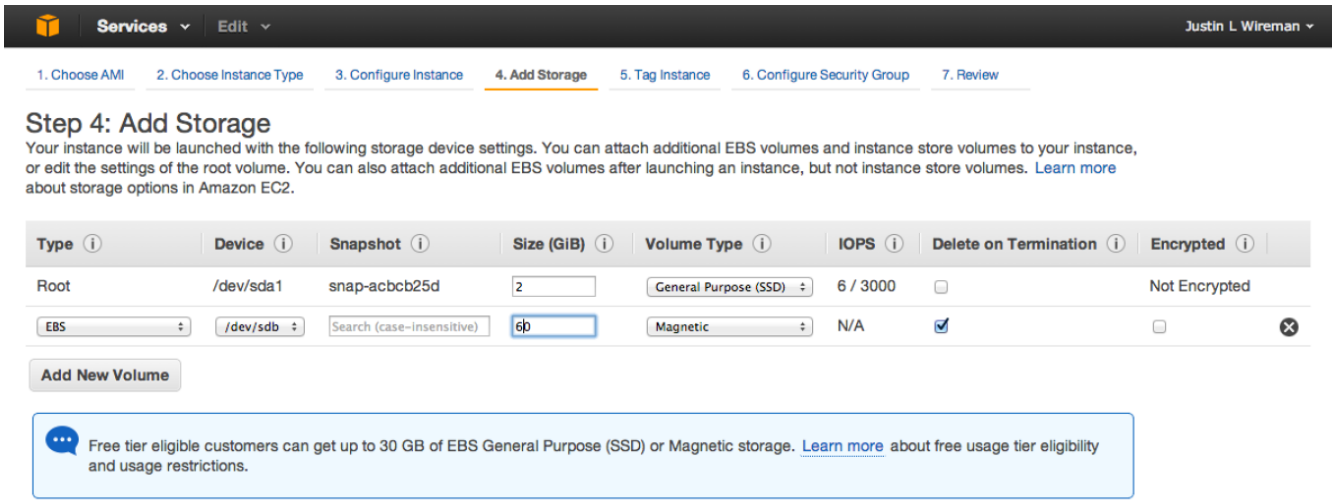
Instance details

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



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.

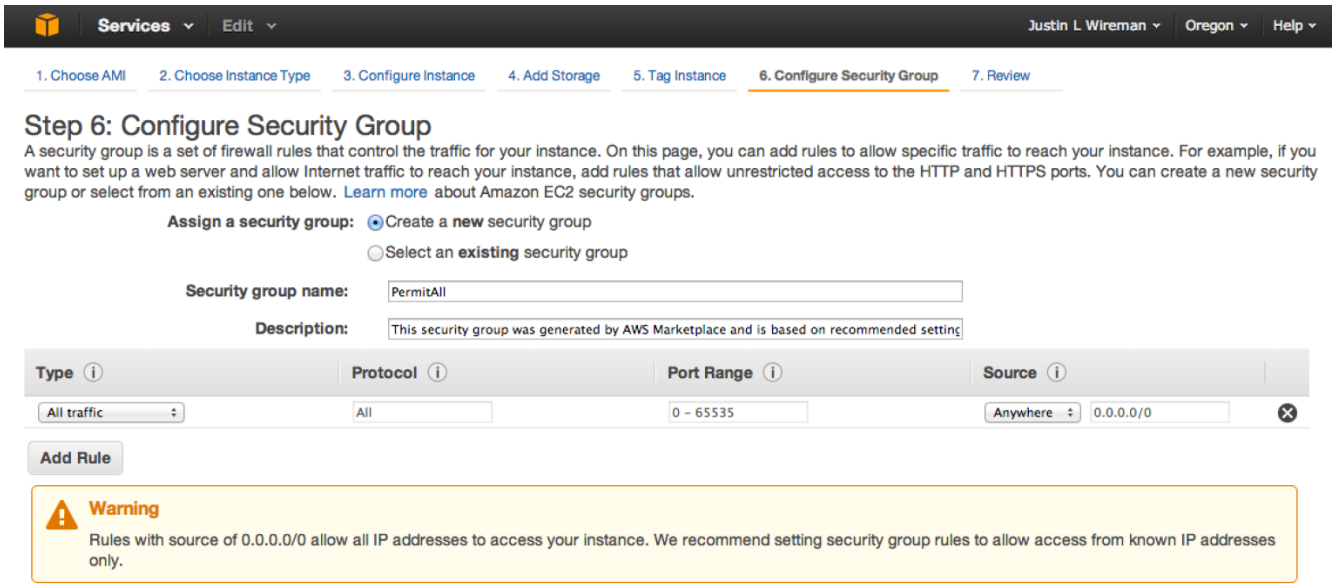


Instance tags

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

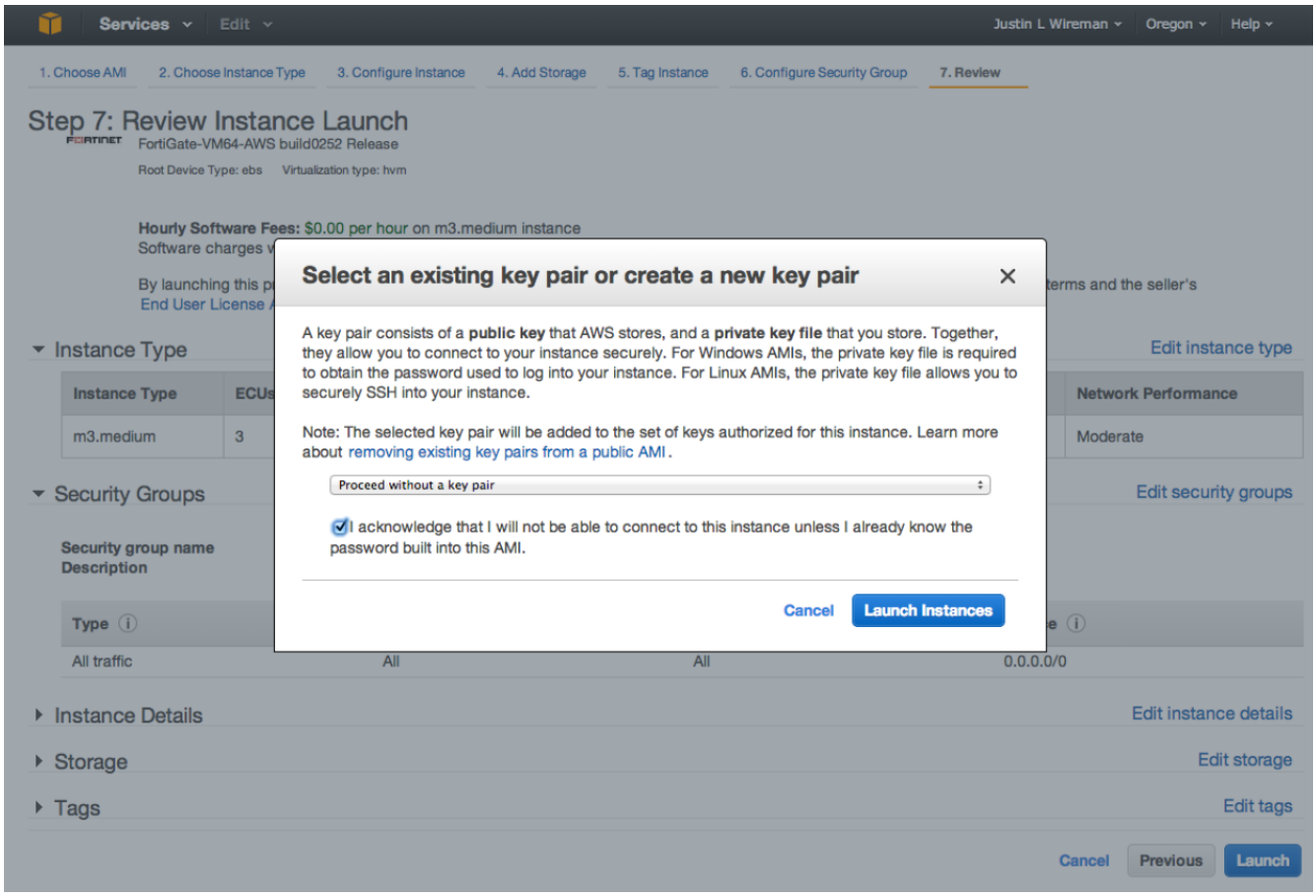
Security groups

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.



Key pair and launching instance

Choose proceed without a keypair and use the default FortiMail username/password, and click Launch Instance to begin trhe provisioning.


Services
Edit
Justin L Wireman
Oregon
Help
1. Choose AMI
2. Choose Instance Type
3. Configure Instance
4. Add Storage
5. Tag Instance
6. Configure Security Group
7. Review
Step 7: Review Instance Launch
FortiGate-VM64-AWS build0252 Release
Root Device Type: ebs
Virtualization type: hvm
Hourly Software Fees: $0.00 per hour on m3.medium instance
Select an existing key pair or create a new key pair
A key pair consists of a public key that AWS stores, and a private key file that you store. Together, they allow you to connect to your instance securely. For Windows AMIs, the private key file is required to obtain the password used to log into your instance. For Linux AMIs, the private key file allows you to securely SSH into your instance.
Note: The selected key pair will be added to the set of keys authorized for this instance. Learn more about removing existing key pairs from a public AMI.
Proceed without a key pair
I acknowledge that I will not be able to connect to this instance unless I already know the password built into this AMI.
Cancel
Launch Instances
Instance Type
Edit instance type
Instance Type
ECUs
Network Performance
m3.medium
3
Moderate
Security Groups
Edit security groups
Security group name
Description
Type
All traffic
All
All
0.0.0.0/0
Instance Details
Edit instance details
Storage
Edit storage
Tags
Edit tags
Cancel
Previous
Launch

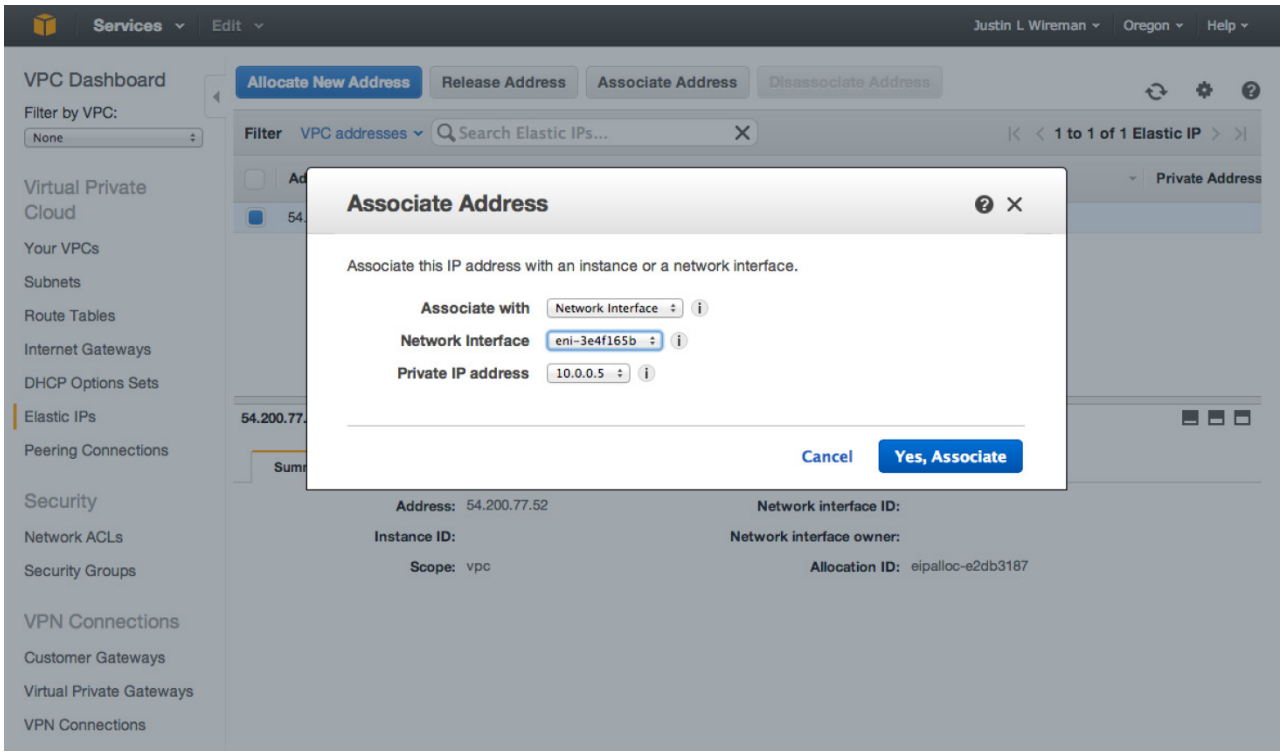
Network Configuration

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.

Configuring AWS network settings

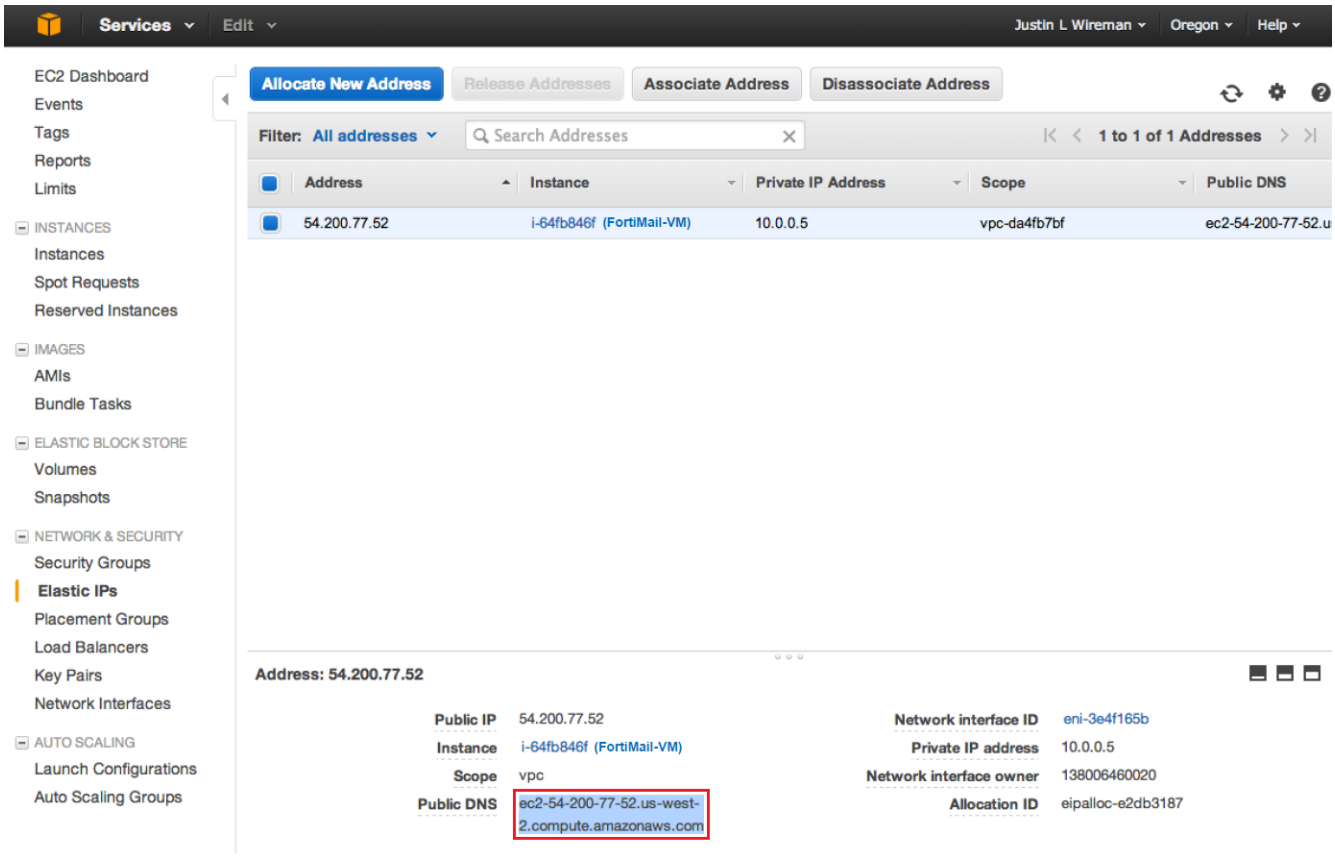
Associate a public “elastic” IP to the FE-VM public interface.

1. On the EC2 Dashboard under the Network interface menu.
   - Locate the public interface ENI (see Setting up the default route for the private network on page 21 for a screenshot of this menu).
2. 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.



Confirming the assigned public address

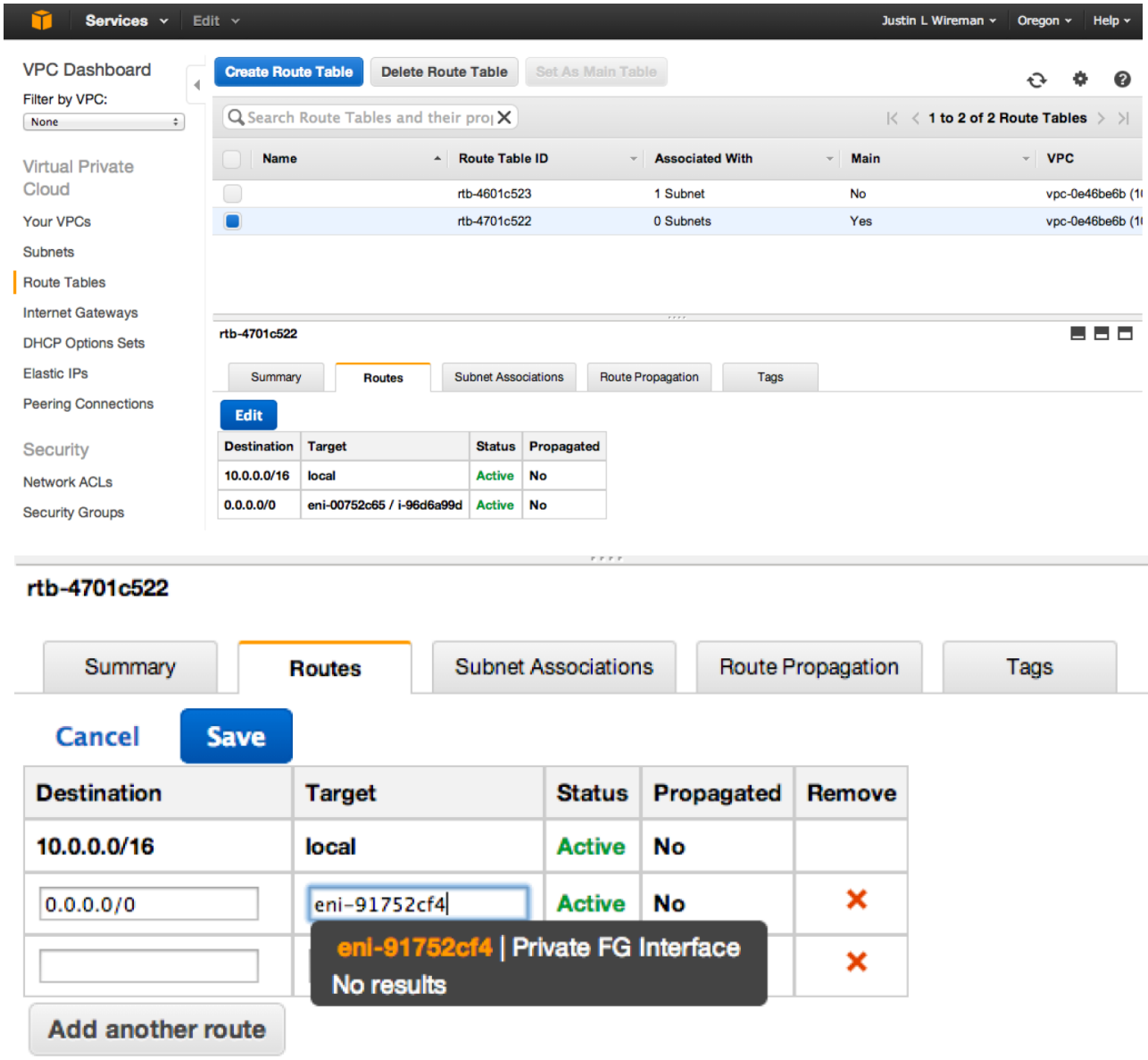
Take note of the public IP address and DNS assigned. You will use these items in later steps.



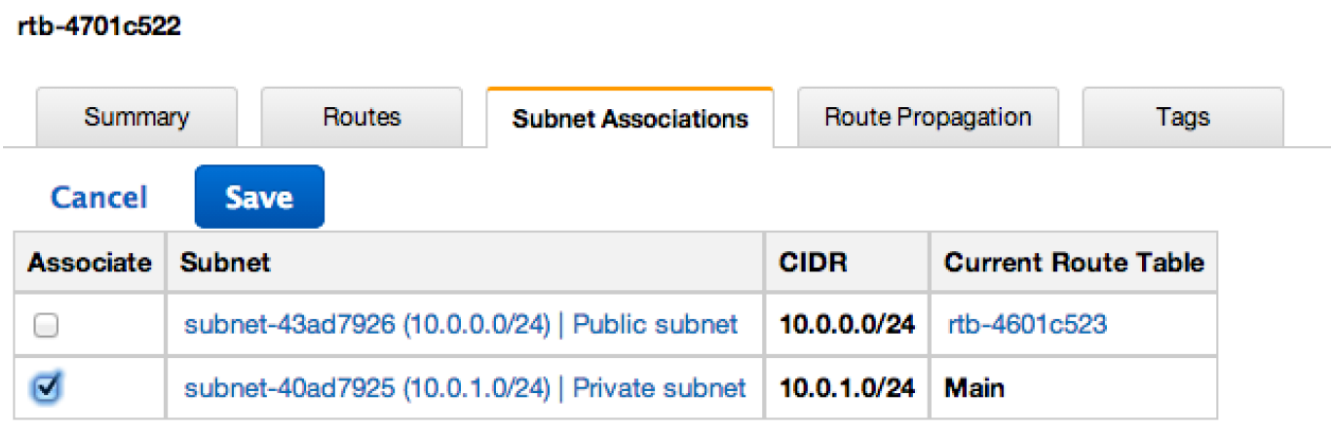
Setting up the default route for the private network

1. On the EC2 Dashboard under the Network interface menu.
   - Locate the network interface ID (ENI-) of the private network and Copy the ID.
2. 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.



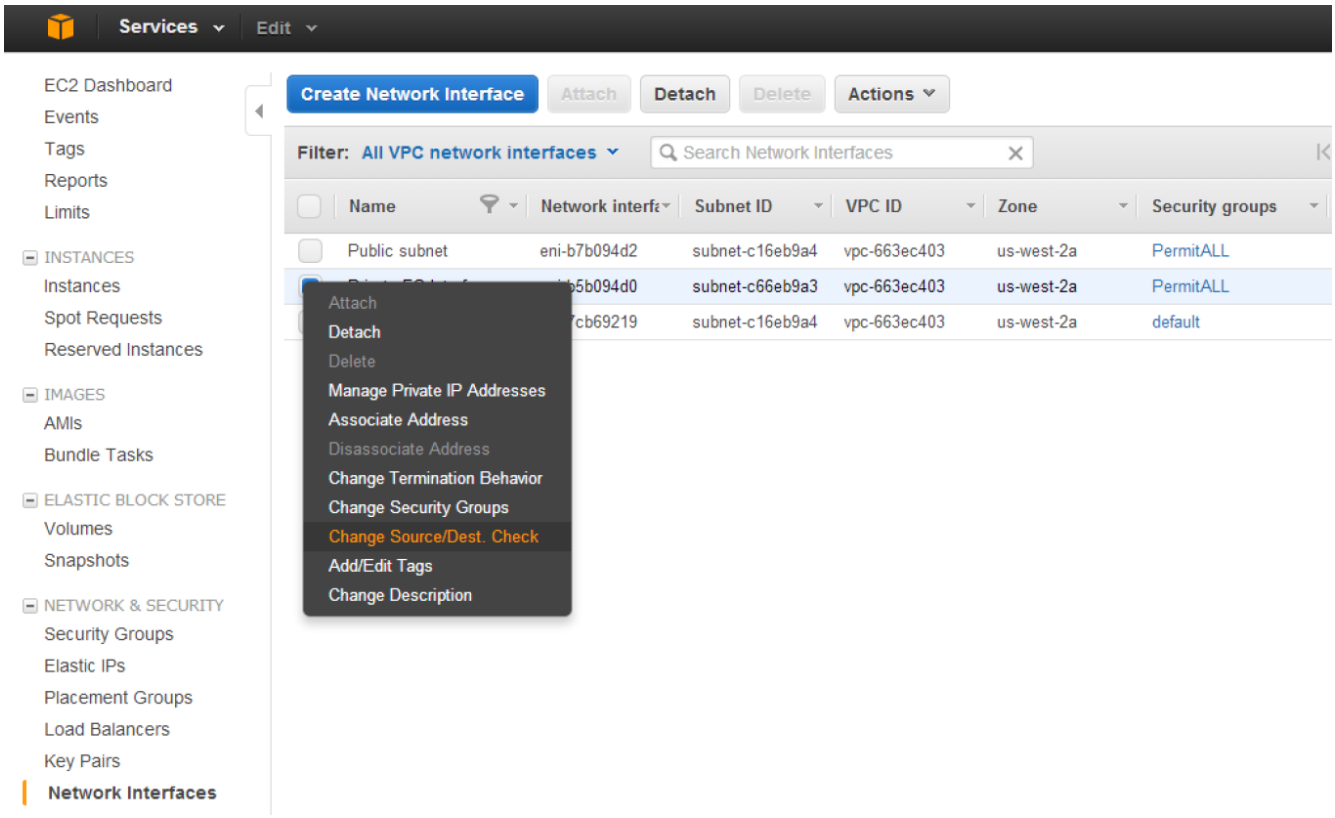
3. Associate the private subnet to the private routing entry you have been editing in the previous steps.



Disabling 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.

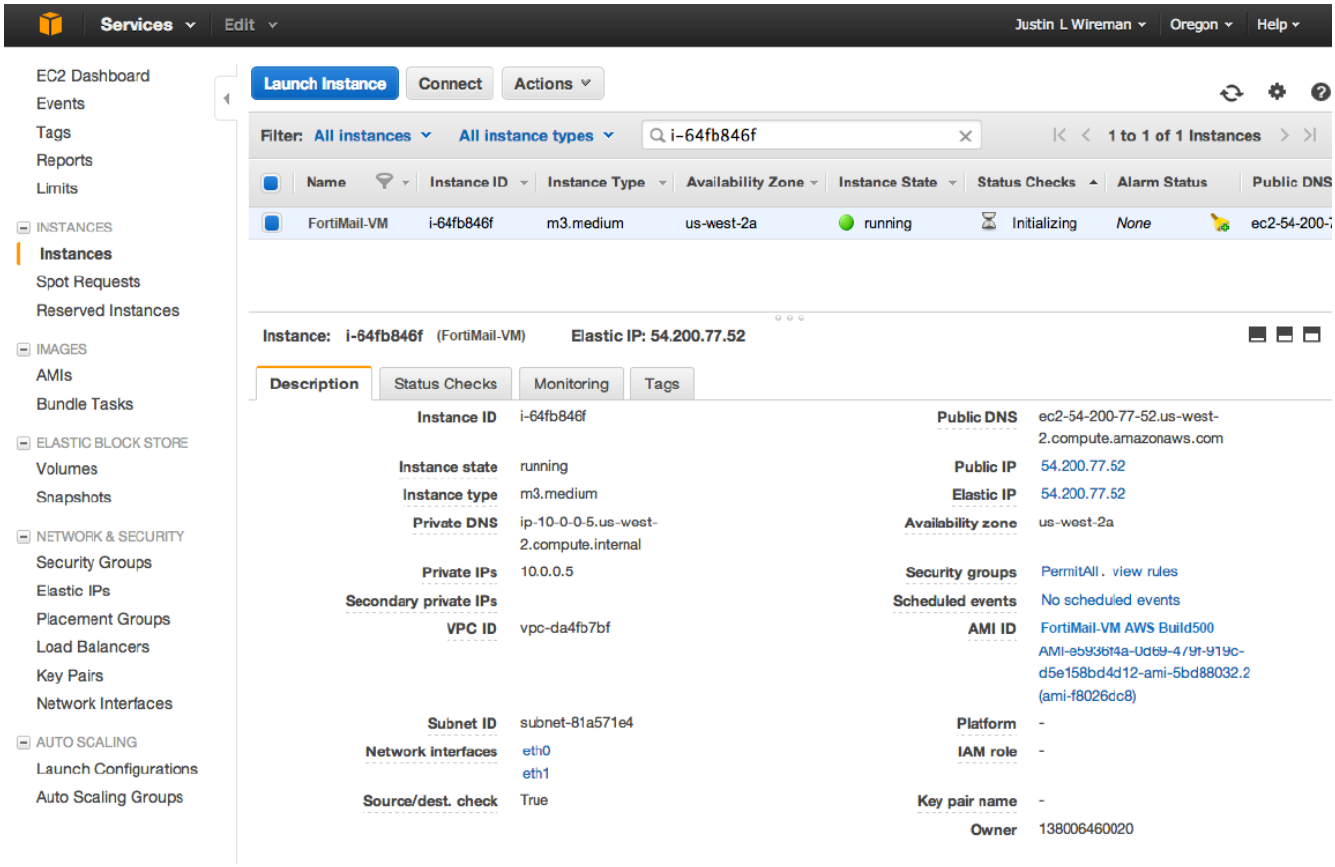
Select Disable and Save.



Navigating to EC2 dash to review the instance state

Once you confirm that the instance has finished provisioning and powering up, check the following items:

- Public IP/DNS assigned
- Confirm the correct security group is assigned



Accessing the virtual FortiMail

Open an 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)

SSH to the FortiMail unit

SSH to the device using the public IP address or the DNS hostname.

Issue the following command to test access:

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

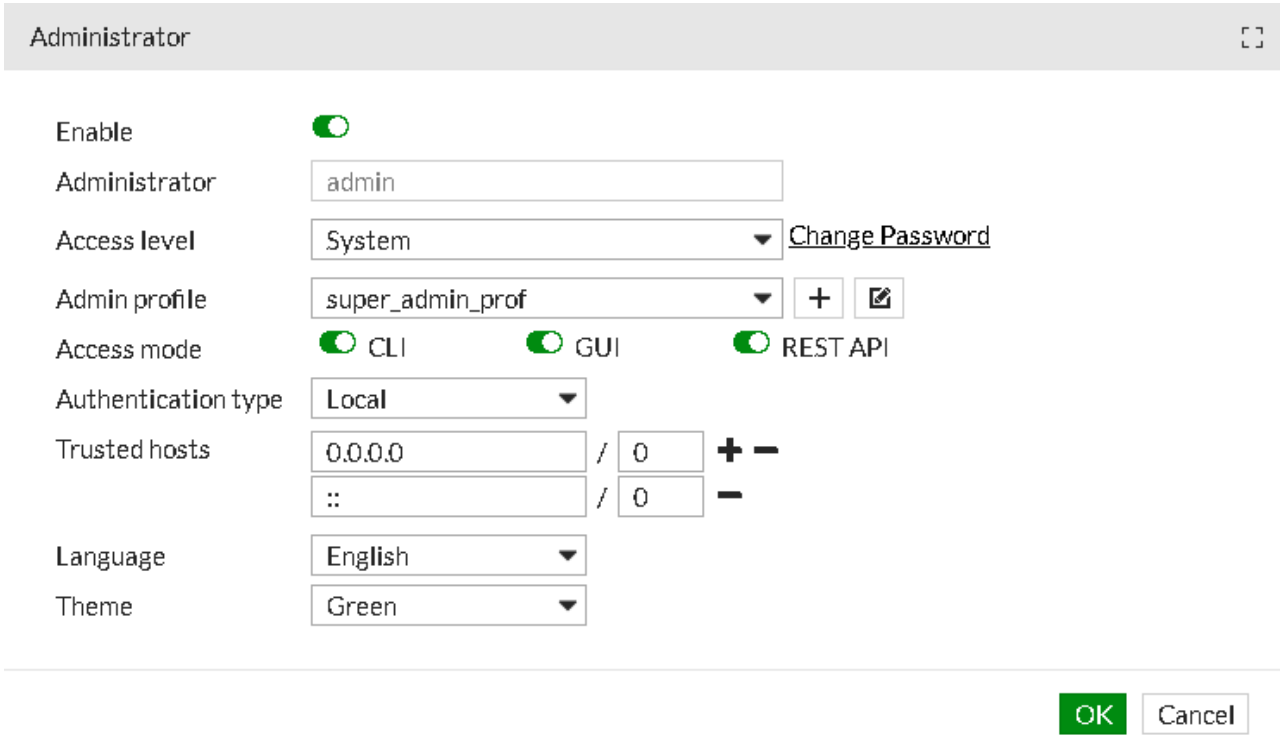
FortiMail Configuration

After you log on to FortiMail, you can start to configure the system. For more information, see the FortiMail Administration Guide.

Updating the administrator password

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

1. Go to *System* > *Administrator* > *Administrator*.
2. Edit the admin user and enter an appropriate password. The admin user does not have a password by default.



Installing the license

In the *License Information* widget on the FortiMail VM web-based manager (under *Dashboard* > *Status*), click the *Upload* link to the right of *VM*, and upload the license.

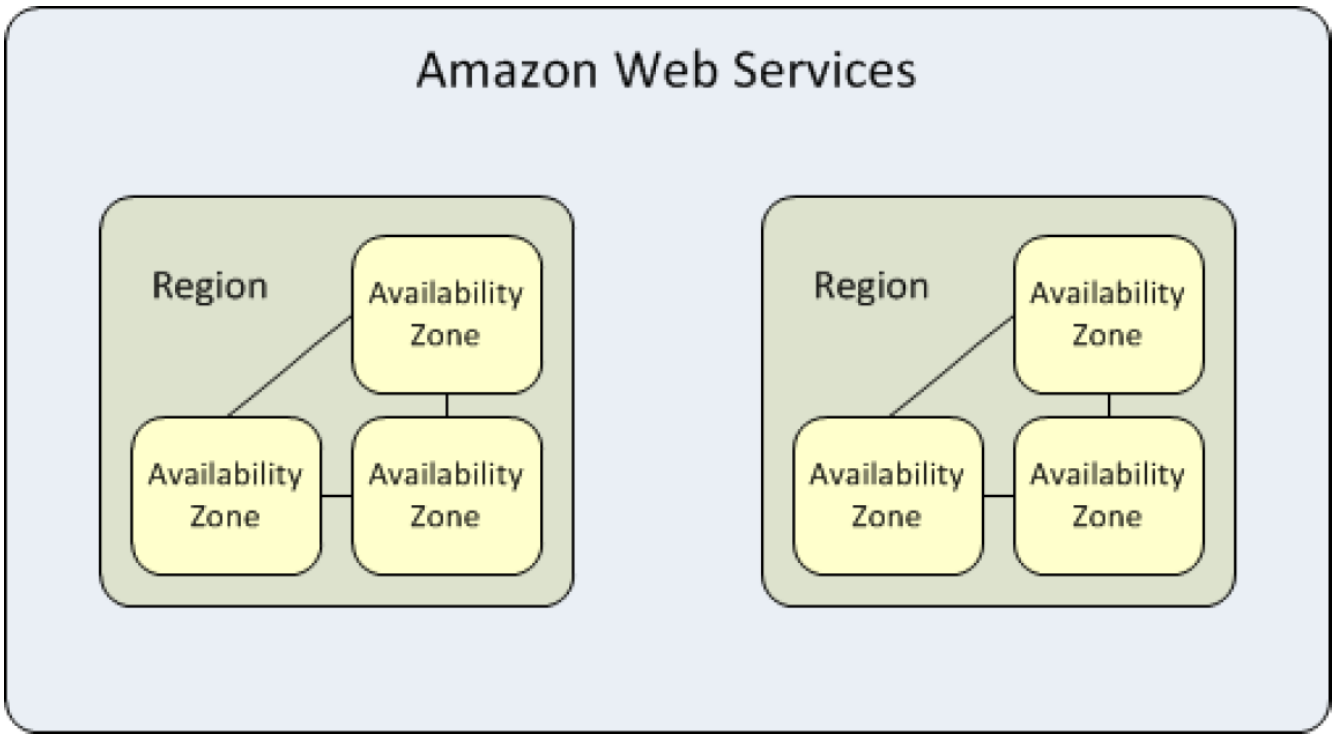
Appendix

The following section includes the following:

Regions and Availability Zones

The following section includes 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.

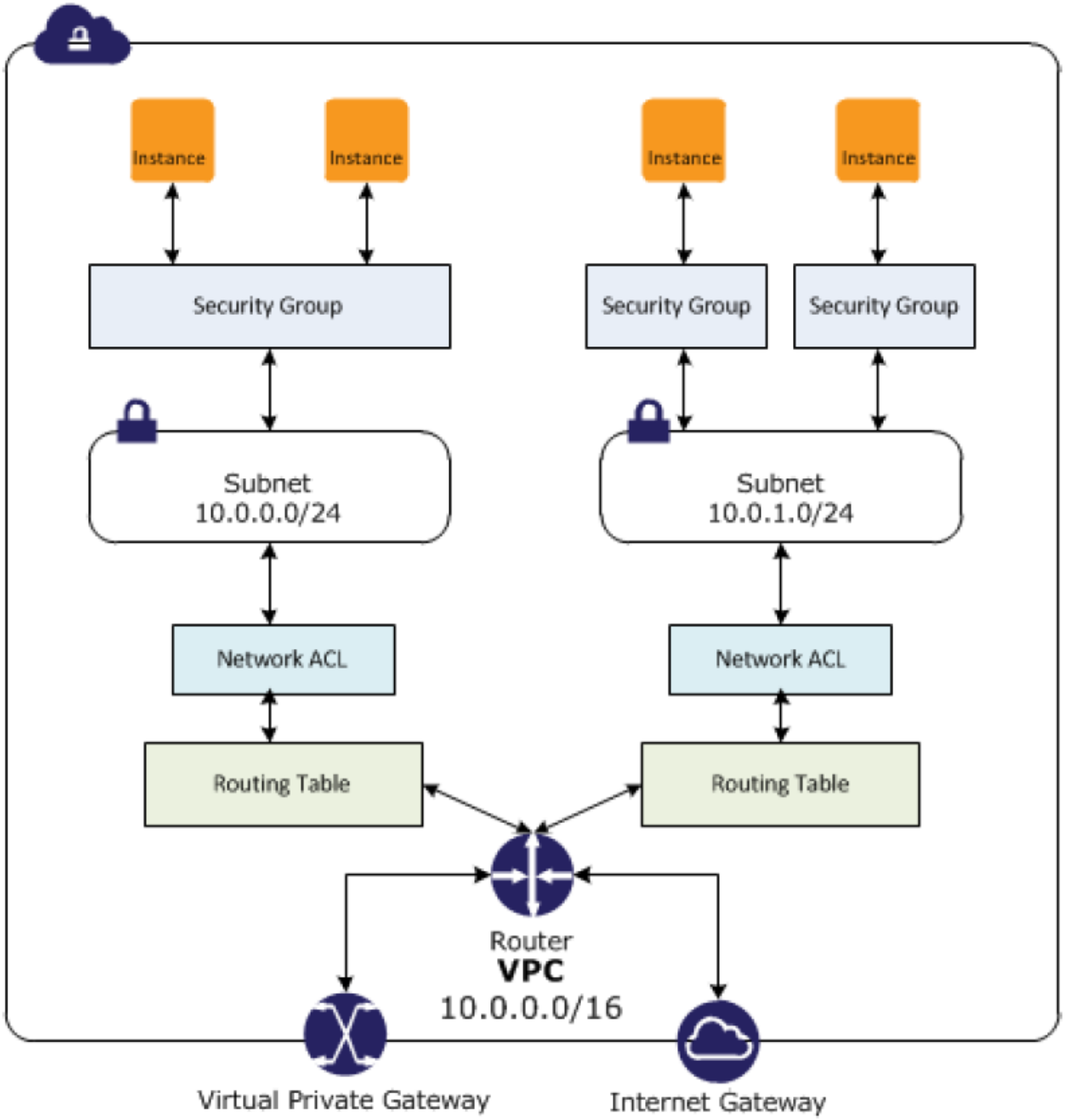
Each key pair requires a name. Be sure to choose a name that is easy to remember. Amazon EC2 associates the public key with the name that you specify as the key name. Amazon EC2 stores the public key only, and you store the private key. Anyone who possesses your private key can decrypt your login information, 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 information and links

- https://docs.aws.amazon.com/vpc/
- https://docs.aws.amazon.com/vpc/latest/userguide/what-is-amazon-vpc.html

www.fortinet.com