



# 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](mailto:techdoc@fortinet.com)

October 18, 2024

FortiMail 7.6.0 AWS Deployment Guide

06-760-000000-20241018

# TABLE OF CONTENTS

<b>Change Log</b> .....	<b>4</b>
<b>Overview</b> .....	<b>5</b>
Amazon Virtual Private Cloud (VPC) .....	5
Components of Amazon VPC .....	6
Network information .....	6
<b>Basic AWS Network Setup</b> .....	<b>8</b>
Setting up your AWS account .....	8
Creating a Virtual Private Cloud (VPC) .....	8
VPC Wizard .....	9
<b>FortiMail Provisioning</b> .....	<b>13</b>
EC2 launching virtual machines .....	13
Choosing an AMI .....	13
Instance type .....	15
Instance details .....	16
Instance storage .....	16
Instance tags .....	17
Security groups .....	17
Key pair and launching instance .....	18
<b>Network Configuration</b> .....	<b>20</b>
Configuring AWS network settings .....	20
Confirming the assigned public address .....	20
Setting up the default route for the private network .....	21
Disabling Source/Destination check on the private FortiMail interface .....	23
Navigating to EC2 dash to review the instance state .....	23
Accessing the virtual FortiMail .....	24
SSH to the FortiMail unit .....	24
<b>FortiMail Configuration</b> .....	<b>25</b>
Updating the administrator password .....	25
Installing the license .....	25
<b>Appendix</b> .....	<b>26</b>
Regions and Availability Zones .....	26
Amazon EC2 key pairs .....	27
Detailed VPC diagram .....	28
Additional information and links .....	29

# Change Log

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

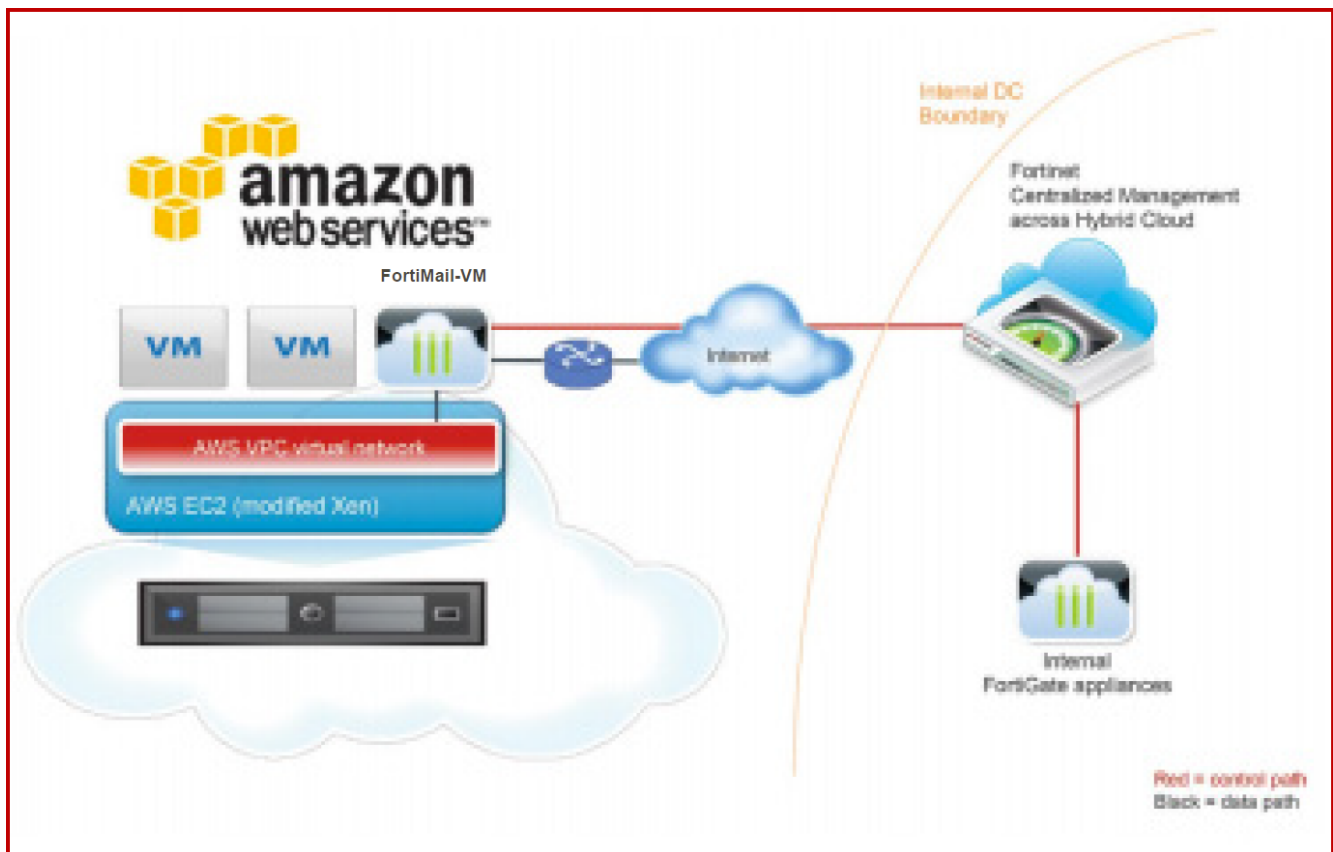
# Overview

This document is designed to be a quick start walk-through 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?

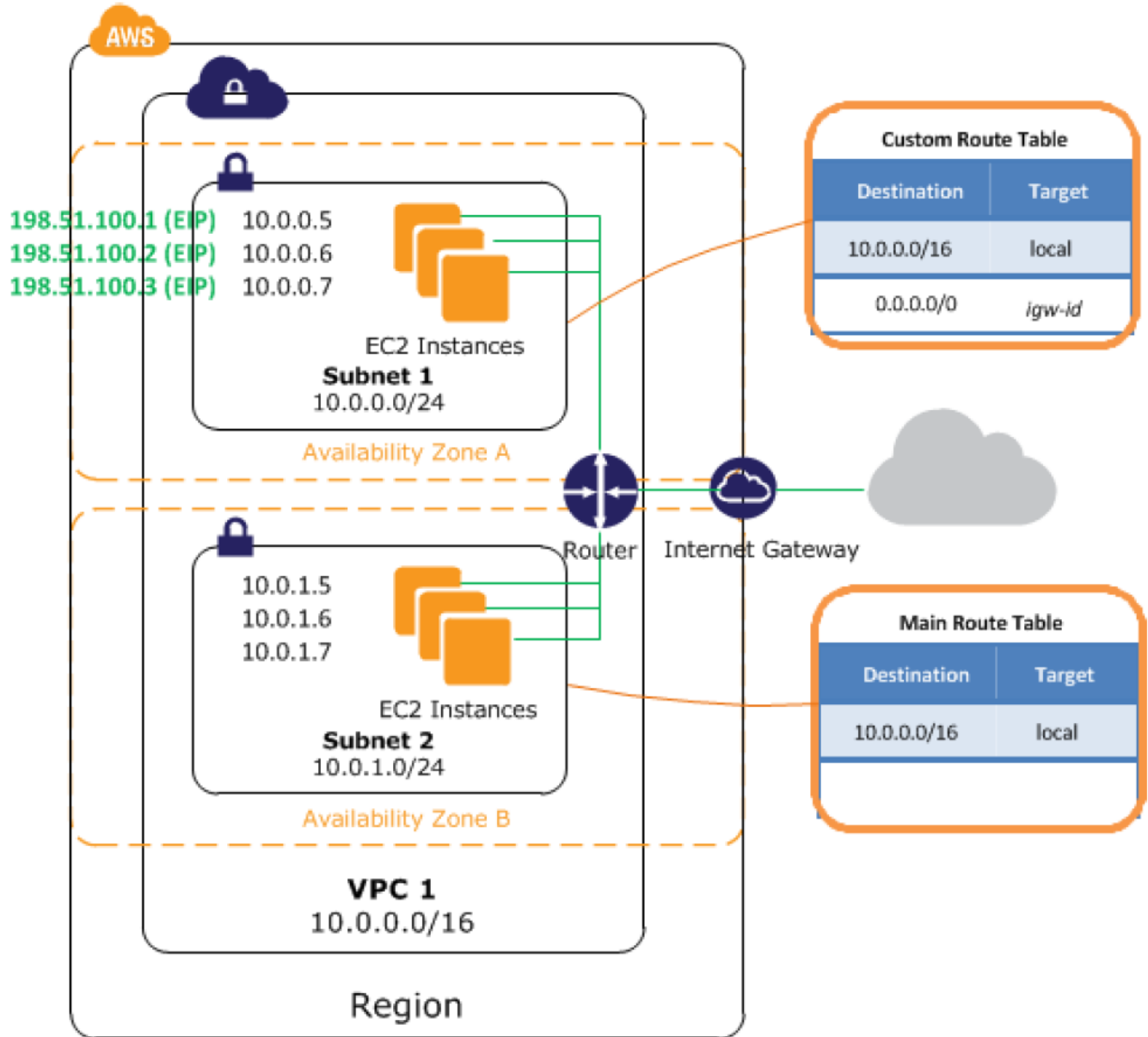
Instances without EIPs can access the Internet in one of two ways:

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



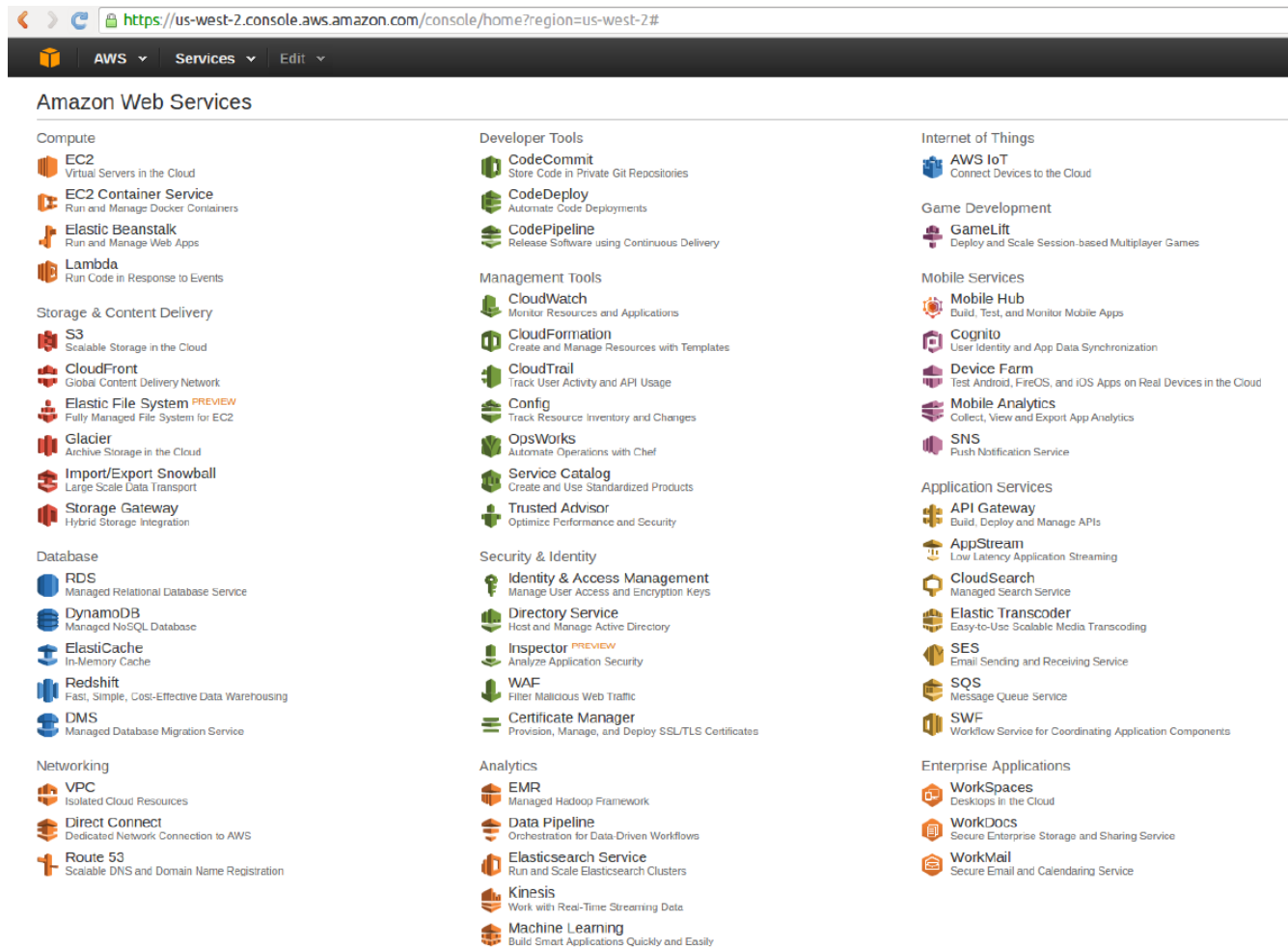
**Warning:** AWS blocks outbound traffic on port 25 (SMTP) of all EC2 instances by default. For information about how to remove the restriction, see:

<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.

0 Running Instances

0 Elastic IPs

0 Dedicated Hosts

0 Snapshots

1 Volumes

0 Load Balancers

1 Key Pairs

1 Security Groups

0 Placement Groups

Easily deploy Ruby, PHP, Java, .NET, Python, Node.js & Docker applications with Elastic Beanstalk.

### Create Instance

To start using Amazon EC2 you will want to launch a virtual server, known as an Amazon EC2 instance.

[Launch Instance](#)

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

### Service Health

**Service Status:**

- US West (Oregon): This service is operating normally

**Availability Zone Status:**

- us-west-2a: Availability zone is operating normally
- us-west-2b: Availability zone is operating normally
- us-west-2c: Availability zone is operating normally

[Service Health Dashboard](#)

### Scheduled Events

**US West (Oregon):**

No events



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.

Browser address bar: <https://us-west-2.console.aws.amazon.com/vpc/home?region=us-west-2#wizardSelector:>

AWS Services Edit

### Step 1: Select a VPC Configuration

**VPC with a Single Public Subnet**

VPC with Public and Private Subnets

VPC with Public and Private Subnets and Hardware VPN Access

VPC with a Private Subnet Only and Hardware VPN Access

Your instances run in a private, isolated section of the AWS cloud with direct access to the Internet. Network access control lists and security groups can be used to provide strict control over inbound and outbound network traffic to your instances.

**Creates:**

A /16 network with a /24 subnet. Public subnet instances use Elastic IPs or Public IPs to access the Internet.

[Select](#)

Browser address bar: <https://us-west-2.console.aws.amazon.com/vpc/home?region=us-west-2#wizardSelector:>

AWS Services Edit

### Step 1: Select a VPC Configuration

VPC with a Single Public Subnet

**VPC with Public and Private Subnets**

VPC with Public and Private Subnets and Hardware VPN Access

VPC with a Private Subnet Only and Hardware VPN Access

In addition to containing a public subnet, this configuration adds a private subnet whose instances are not addressable from the Internet. Instances in the private subnet can establish outbound connections to the Internet via the public subnet using Network Address Translation (NAT).

**Creates:**

A /16 network with two /24 subnets. Public subnet instances use Elastic IPs to access the Internet. Private subnet instances access the Internet via Network Address Translation (NAT). (Hourly charges for NAT devices apply.)

[Select](#)

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.

The screenshot shows the AWS Management Console interface for configuring a VPC. The browser address bar displays the URL: <https://us-west-2.console.aws.amazon.com/vpc/home?region=us-west-2#wizardFullpagePublicAndPrivate:>. The navigation bar includes the AWS logo, 'AWS', 'Services', and 'Edit' menus.

### Step 2: VPC with Public and Private Subnets

---

**IP CIDR block:**  (65531 IP addresses available)  
**VPC name:**

---

**Public subnet:**  (251 IP addresses available)  
**Availability Zone:**   
**Public subnet name:**   
**Private subnet:**  (251 IP addresses available)  
**Availability Zone:**   
**Private subnet name:**

You can add more subnets after AWS creates the VPC.

---

Specify the details of your NAT instance ([Instance rates apply](#)).

**Instance type:**   
**Key pair name:**

---

Add endpoints for S3 to your subnets

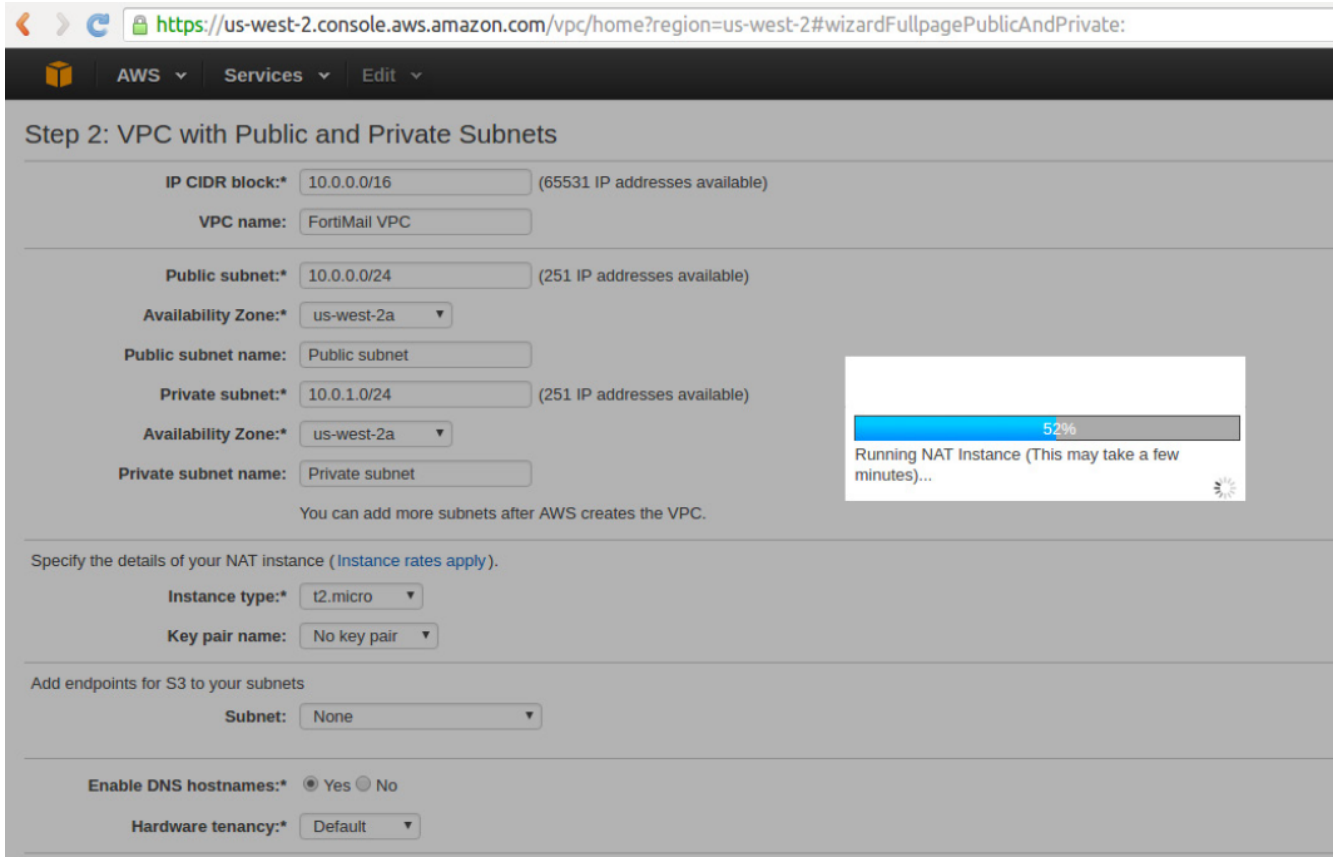
**Subnet:**

---

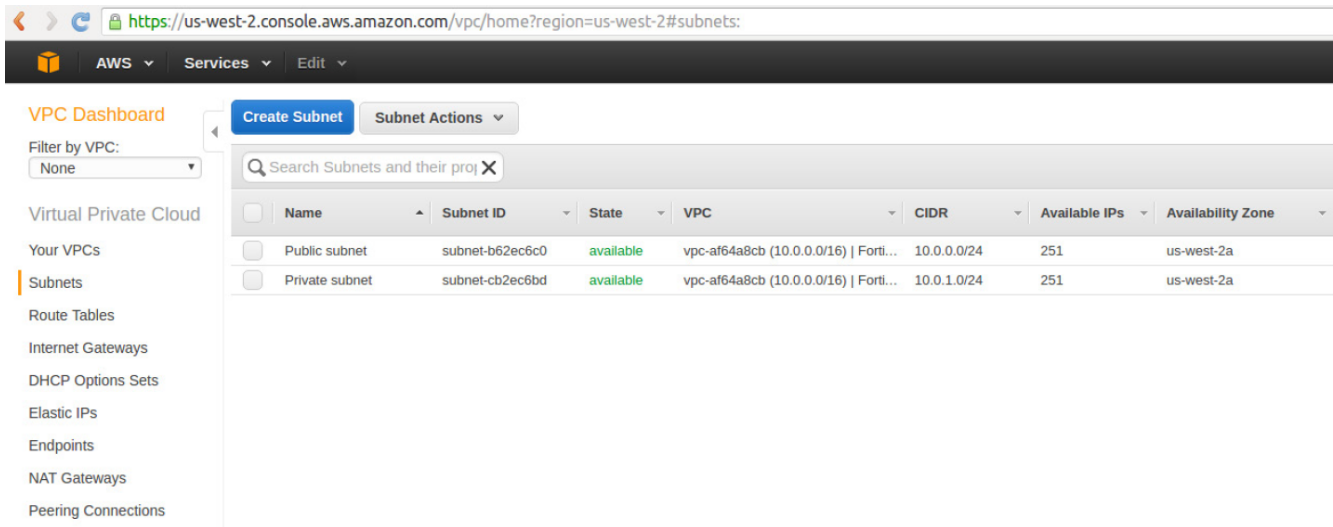
**Enable DNS hostnames:**  Yes  No  
**Hardware tenancy:**

---

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.

The screenshot shows the AWS Management Console for the EC2 dashboard in the us-west-2 region. The top navigation bar includes the AWS logo, 'Services', and 'Edit' options. The left sidebar contains a navigation menu with categories like EC2 Dashboard, INSTANCES, IMAGES, ELASTIC BLOCK STORE, NETWORK & SECURITY, LOAD BALANCING, and AUTO SCALING. The main content area displays a summary of resources: 0 Running Instances, 0 Dedicated Hosts, 1 Volumes, 1 Key Pairs, 0 Placement Groups, 0 Elastic IPs, 0 Snapshots, 0 Load Balancers, and 1 Security Groups. A blue banner promotes Elastic Beanstalk. Below this is the 'Create Instance' section with a 'Launch Instance' button and a note about the region. The 'Service Health' section shows that the US West (Oregon) service is operating normally, and all three availability zones (us-west-2a, us-west-2b, us-west-2c) are also operating normally. A 'Scheduled Events' section shows no events for the region.

## 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)

Fortinet FortiAnalyzer-VM securely aggregates log data from Fortinet devices and other syslog-compatible devices, using a comprehensive suite of easy-customized reports, ...

[More info](#)

**FORTINET** **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** **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** **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** **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](#)

### Fortinet FortiMail-VM (BYOL)



#### Fortinet FortiMail-VM (BYOL)

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 - including advanced malware -, as well as outbound threats and data loss with a wide range of top-rated security capabilities. These capabilities cover: antispam, antiphishing, ...

[More info](#)

[Learn more on AWS Marketplace](#)

#### Product Details

<b>Sold by</b>	Fortinet, Inc.
<b>Customer Rating</b>	★★★★★ (0)
<b>Latest Version</b>	v5.3.1
<b>Base Operating System</b>	Linux/Unix, Other v5.3.1
<b>Delivery Method</b>	64-bit Amazon Machine Image (AMI)
<b>License Agreement</b>	<a href="#">End User License Agreement</a>

#### Pricing Details

#### Bring Your Own License (BYOL)

#### Hourly Fees

Instance Type	Software	EC2	Total
M3 Medium	\$0.00	\$0.067	<b>\$0.067/hr</b>
M3 Large	\$0.00	\$0.133	<b>\$0.133/hr</b>
M3 Extra Large	\$0.00	\$0.266	<b>\$0.266/hr</b>
M3 Double Extra Large	\$0.00	\$0.532	<b>\$0.532/hr</b>
C3 Large	\$0.00	\$0.105	<b>\$0.105/hr</b>
C3 Extra Large	\$0.00	\$0.21	<b>\$0.21/hr</b>
C3 Double Extra Large	\$0.00	\$0.42	<b>\$0.42/hr</b>
C4 Large	\$0.00	\$0.105	<b>\$0.105/hr</b>
C4 Extra Large	\$0.00	\$0.209	<b>\$0.209/hr</b>
C4 Double Extra Large	\$0.00	\$0.419	<b>\$0.419/hr</b>
M4 Large	\$0.00	\$0.12	<b>\$0.12/hr</b>
M4 Extra Large	\$0.00	\$0.239	<b>\$0.239/hr</b>
M4 Double Extra Large	\$0.00	\$0.479	<b>\$0.479/hr</b>

#### EBS Magnetic volumes

\$0.05 per GB-month of provisioned storage  
\$0.05 per 1 million I/O requests

You will not be charged until you launch this instance.

[Cancel](#)

[Continue](#)

## Instance type

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

1. Choose AMI
2. Choose Instance Type
3. Configure Instance
4. Add Storage
5. Tag Instance
6. Configure Security Group
7. Review

#### Step 2: Choose an Instance Type

Amazon EC2 provides a wide selection of instance types optimized to fit different use cases. Instances are virtual servers that can run applications. They have varying combinations of CPU, memory, storage, and networking capacity, and give you the flexibility to choose the appropriate mix of resources for your applications. [Learn more](#) about instance types and how they can meet your computing needs.

Filter by: [All instance types](#) [Current generation](#) [Show/Hide Columns](#)

Currently selected: m3.medium (3 ECUs, 1 vCPUs, 2.5 GHz, Intel Xeon E5-2670v2, 3.75 GiB memory, 1 x 4 GiB Storage Capacity)

Note: The vendor recommends using a m3.medium instance (or larger) for the best experience with this product.

	Family	Type	vCPUs	Memory (GiB)	Instance Storage (GB)	EBS-Optimized Available	Network Performance
<input checked="" type="radio"/>	General purpose	t2.nano	1	0.5	EBS only	-	Low to Moderate
<input checked="" type="radio"/>	General purpose	t2.micro	1	1	EBS only	-	Low to Moderate
<input checked="" type="radio"/>	General purpose	t2.small	1	2	EBS only	-	Low to Moderate
<input checked="" type="radio"/>	General purpose	t2.medium	2	4	EBS only	-	Low to Moderate
<input checked="" type="radio"/>	General purpose	t2.large	2	8	EBS only	-	Low to Moderate
<input type="radio"/>	General purpose	m4.large	2	8	EBS only	Yes	Moderate
<input type="radio"/>	General purpose	m4.xlarge	4	16	EBS only	Yes	High
<input type="radio"/>	General purpose	m4.2xlarge	8	32	EBS only	Yes	High
<input checked="" type="radio"/>	General purpose	m4.4xlarge	16	64	EBS only	Yes	High
<input checked="" type="radio"/>	General purpose	m4.10xlarge	40	160	EBS only	Yes	10 Gigabit
<input checked="" type="radio"/>	General purpose	m3.medium	1	3.75	1 x 4 (SSD)	-	Moderate
<input type="radio"/>	General purpose	m3.large	2	7.5	1 x 32 (SSD)	-	Moderate
<input type="radio"/>	General purpose	m3.xlarge	4	15	2 x 40 (SSD)	Yes	High

[Cancel](#) [Previous](#) [Review and Launch](#) [Next: Configure Instance Details](#)

## Instance details

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

- 1. Choose AMI
- 2. Choose Instance Type
- 3. Configure Instance
- 4. Add Storage
- 5. Tag Instance
- 6. Configure Security Group
- 7. Review

### Step 3: Configure Instance Details

**Number of instances** ⓘ

---

**Purchasing option** ⓘ  Request Spot Instances

---

**Network** ⓘ  ↻ Create new VPC

**Subnet** ⓘ  Create new subnet  
 250 IP Addresses available

**Auto-assign Public IP** ⓘ

---

**IAM role** ⓘ

---

**Shutdown behavior** ⓘ

**Enable termination protection** ⓘ  Protect against accidental termination

**Monitoring** ⓘ  Enable CloudWatch detailed monitoring  
 Additional charges apply.

**Tenancy** ⓘ   
 Additional charges will apply for dedicated tenancy.

▼ Network interfaces

Device	Network Interface	Subnet	Primary IP	Secondary IP addresses
eth0	<input type="text" value="New network interface"/>	<input type="text" value="subnet-81a571e4"/>	<input type="text" value="10.0.0.5"/>	<a href="#">Add IP</a>
eth1	<input type="text" value="New network interface"/>	<input type="text" value="subnet-86a571e3"/>	<input type="text" value="10.0.1.5"/>	<a href="#">Add IP</a>

[Cancel](#)
[Previous](#)
[Review and Launch](#)

## 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 4: Add Storage**  
 Your instance will be launched with the following storage device settings. You can attach additional EBS volumes and instance store volumes to your instance, or edit the settings of the root volume. You can also attach additional EBS volumes after launching an instance, but not instance store volumes. [Learn more](#) about storage options in Amazon EC2.

Type	Device	Snapshot	Size (GiB)	Volume Type	IOPS	Delete on Termination	Encrypted
Root	/dev/sda1	snap-acbcb25d	2	General Purpose (SSD)	6 / 3000	<input type="checkbox"/>	Not Encrypted
EBS	/dev/sdb	Search (case-insensitive)	6	Magnetic	N/A	<input checked="" type="checkbox"/>	<input type="checkbox"/>

[Add New Volume](#)

Free tier eligible customers can get up to 30 GB of EBS General Purpose (SSD) or Magnetic storage. [Learn more](#) about free usage tier eligibility and usage restrictions.

## Instance tags

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

**Step 5: Tag Instance**  
 A tag consists of a case-sensitive key-value pair. For example, you could define a tag with key = Name and value = Webserver. [Learn more](#) about tagging your Amazon EC2 resources.

Key (127 characters maximum)	Value (255 characters maximum)
Name	FortiMail-VM
Public IP	10.0.0.5
Private IP	10.0.1.5

[Create Tag](#) (Up to 10 tags maximum)

## 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.

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 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

Security group name:

Description:

Type	Protocol	Port Range	Source
All traffic	All	0 - 65535	Anywhere 0.0.0.0/0

Add Rule

**Warning**

Rules with source of 0.0.0.0/0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access from known IP addresses only.

## Key pair and launching instance

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

The screenshot shows the AWS Management Console interface during the 'Step 7: Review Instance Launch' process. The background is dimmed, showing the instance configuration details for a FortiGate-VM64-AWS build0252 Release. A modal dialog box is open in the center, titled 'Select an existing key pair or create a new key pair'. The dialog contains the following text:

**Select an existing key pair or create a new key pair** [X]

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 [v]

I acknowledge that I will not be able to connect to this instance unless I already know the password built into this AMI.

Buttons: Cancel, Launch Instances

The background interface shows the following details:

- 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
- Instance Type: m3.medium, 3 ECUs
- Security Groups: All traffic, All, 0.0.0.0/0
- Buttons: Cancel, Previous, Launch

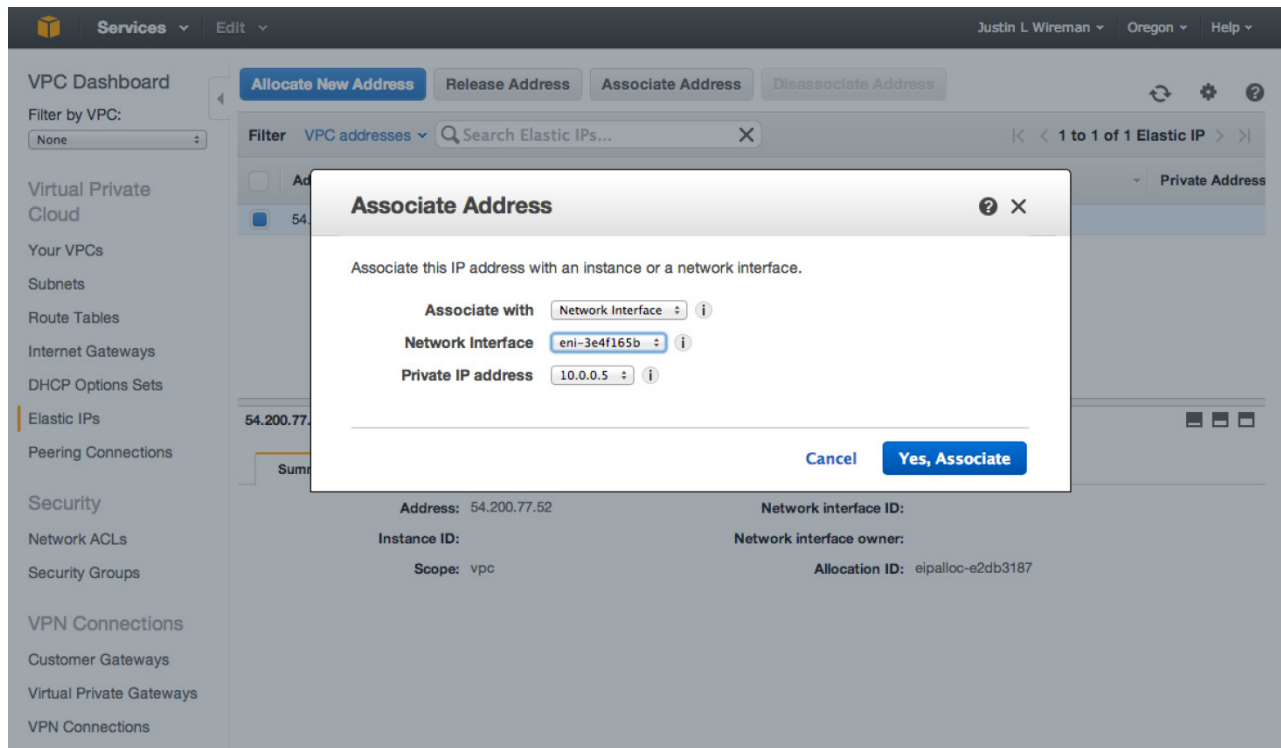
# Network Configuration

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.

The screenshot shows the AWS Management Console interface for Elastic IPs. The left sidebar contains navigation options like EC2 Dashboard, INSTANCES, IMAGES, ELASTIC BLOCK STORE, NETWORK & SECURITY, and AUTO SCALING. The main area shows a table of Elastic IP addresses with columns for Address, Instance, Private IP Address, Scope, and Public DNS. Below the table, detailed information for the selected address (54.200.77.52) is displayed, including its association with instance i-64fb846f and network interface eni-3e4f165b.

Address	Instance	Private IP Address	Scope	Public DNS
54.200.77.52	i-64fb846f (FortiMail-VM)	10.0.0.5	vpc-da4fb7bf	ec2-54-200-77-52.us-west-2.compute.amazonaws.com

<b>Public IP</b>	54.200.77.52	<b>Network interface ID</b>	eni-3e4f165b
<b>Instance</b>	i-64fb846f (FortiMail-VM)	<b>Private IP address</b>	10.0.0.5
<b>Scope</b>	vpc	<b>Network interface owner</b>	138006460020
<b>Public DNS</b>	ec2-54-200-77-52.us-west-2.compute.amazonaws.com	<b>Allocation ID</b>	eipalloc-e2db3187

## 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.

The screenshot shows the AWS Management Console interface for editing a route table. The left sidebar lists navigation options like VPC Dashboard, Virtual Private Cloud, Subnets, and Route Tables. The main content area shows a list of route tables, with 'rtb-4701c522' selected. Below this, the 'Routes' tab is active, displaying a table of routes. The table has columns for Destination, Target, Status, Propagated, and Remove. Two routes are listed: one for 10.0.0.0/16 pointing to 'local', and another for 0.0.0.0/0 pointing to 'eni-00752c65 / i-96d6a99d'. A search box above the table shows 'eni-91752cf4' with a tooltip indicating it is a 'Private FG Interface' with 'No results'.

Destination	Target	Status	Propagated	Remove
10.0.0.0/16	local	Active	No	
0.0.0.0/0	eni-00752c65 / i-96d6a99d	Active	No	✗

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

rtb-4701c522

Summary Routes **Subnet Associations** Route Propagation Tags

Cancel Save

Associate	Subnet	CIDR	Current Route Table
<input type="checkbox"/>	subnet-43ad7926 (10.0.0.0/24)   Public subnet	10.0.0.0/24	rtb-4601c523
<input checked="" type="checkbox"/>	subnet-40ad7925 (10.0.1.0/24)   Private subnet	10.0.1.0/24	Main

## 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.

The screenshot shows the AWS EC2 console interface. On the left is a navigation sidebar with categories like INSTANCES, IMAGES, ELASTIC BLOCK STORE, and NETWORK & SECURITY. The 'Network Interfaces' option is selected. The main panel displays a table of network interfaces. The table has columns for Name, Network interface, Subnet ID, VPC ID, Zone, and Security groups. One interface, 'Private FortiMail', is highlighted in blue. A context menu is open over this interface, listing various actions. The 'Change Source/Dest. Check' option is highlighted in orange.

Name	Network interface	Subnet ID	VPC ID	Zone	Security groups
Public subnet	eni-b7b094d2	subnet-c16eb9a4	vpc-663ec403	us-west-2a	PermitALL
Private FortiMail	eni-b5b094d0	subnet-c66eb9a3	vpc-663ec403	us-west-2a	PermitALL
Private FortiMail	eni-cb69219	subnet-c16eb9a4	vpc-663ec403	us-west-2a	default

## 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

The screenshot shows the AWS Management Console interface. On the left is a navigation menu with categories like INSTANCES, IMAGES, ELASTIC BLOCK STORE, NETWORK & SECURITY, and AUTO SCALING. The main area displays the details for an EC2 instance named 'FortiMail-VM' (ID: i-64fb846f). The instance is in a 'running' state and is initializing. The Elastic IP is 54.200.77.52. Below the instance name, there are tabs for Description, Status Checks, Monitoring, and Tags. The Description tab is active, showing a list of instance attributes and their values.

Attribute	Value	Attribute	Value
Instance ID	i-64fb846f	Public DNS	ec2-54-200-77-52.us-west-2.compute.amazonaws.com
Instance state	running	Public IP	54.200.77.52
Instance type	m3.medium	Elastic IP	54.200.77.52
Private DNS	ip-10-0-0-5.us-west-2.compute.internal	Availability zone	us-west-2a
Private IPs	10.0.0.5	Security groups	PermitAll . view rules
Secondary private IPs		Scheduled events	No scheduled events
VPC ID	vpc-da4fb7bf	AMI ID	FortiMail-VM AWS Build500 AMI-8b93614a-Ud69-4/9f-919c-d5e158bd4d12-ami-5bd88032.2 (ami-f8026dc8)
Subnet ID	subnet-81a571e4	Platform	-
Network interfaces	eth0 eth1	IAM role	-
Source/dest. check	True	Key pair name	-
		Owner	138006460020

## 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.

Administrator ✕

Enable	<input checked="" type="checkbox"/>
Administrator	<input type="text" value="admin"/>
Access level	<input type="text" value="System"/> <span>▼</span> <a href="#">Change Password</a>
Admin profile	<input type="text" value="super_admin_prof"/> <span>▼</span> <input type="button" value="+"/> <input type="button" value="✎"/>
Access mode	<input checked="" type="checkbox"/> CLI <input checked="" type="checkbox"/> GUI <input checked="" type="checkbox"/> REST API
Authentication type	<input type="text" value="Local"/> <span>▼</span>
Trusted hosts	<input type="text" value="0.0.0.0"/> / <input type="text" value="0"/> <input type="button" value="+"/> <input type="button" value="-"/> <input type="text" value="::"/> / <input type="text" value="0"/> <input type="button" value="-"/>
Language	<input type="text" value="English"/> <span>▼</span>
Theme	<input type="text" value="Green"/> <span>▼</span>

---

## 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

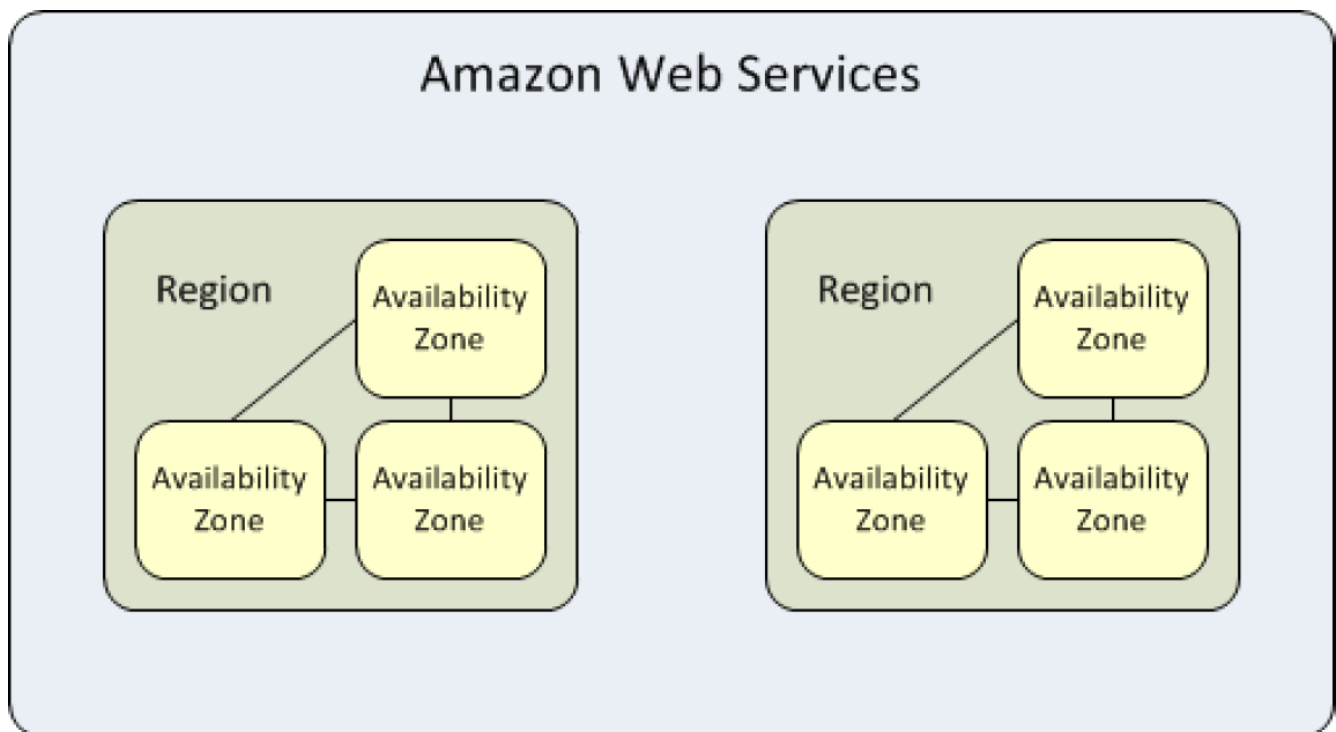
The following section includes the following:

- [Regions and Availability Zones on page 26](#)
- [Amazon EC2 key pairs on page 27](#)
- [Detailed VPC diagram on page 28](#)
- [Additional information and links on page 29](#)

## 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](#).

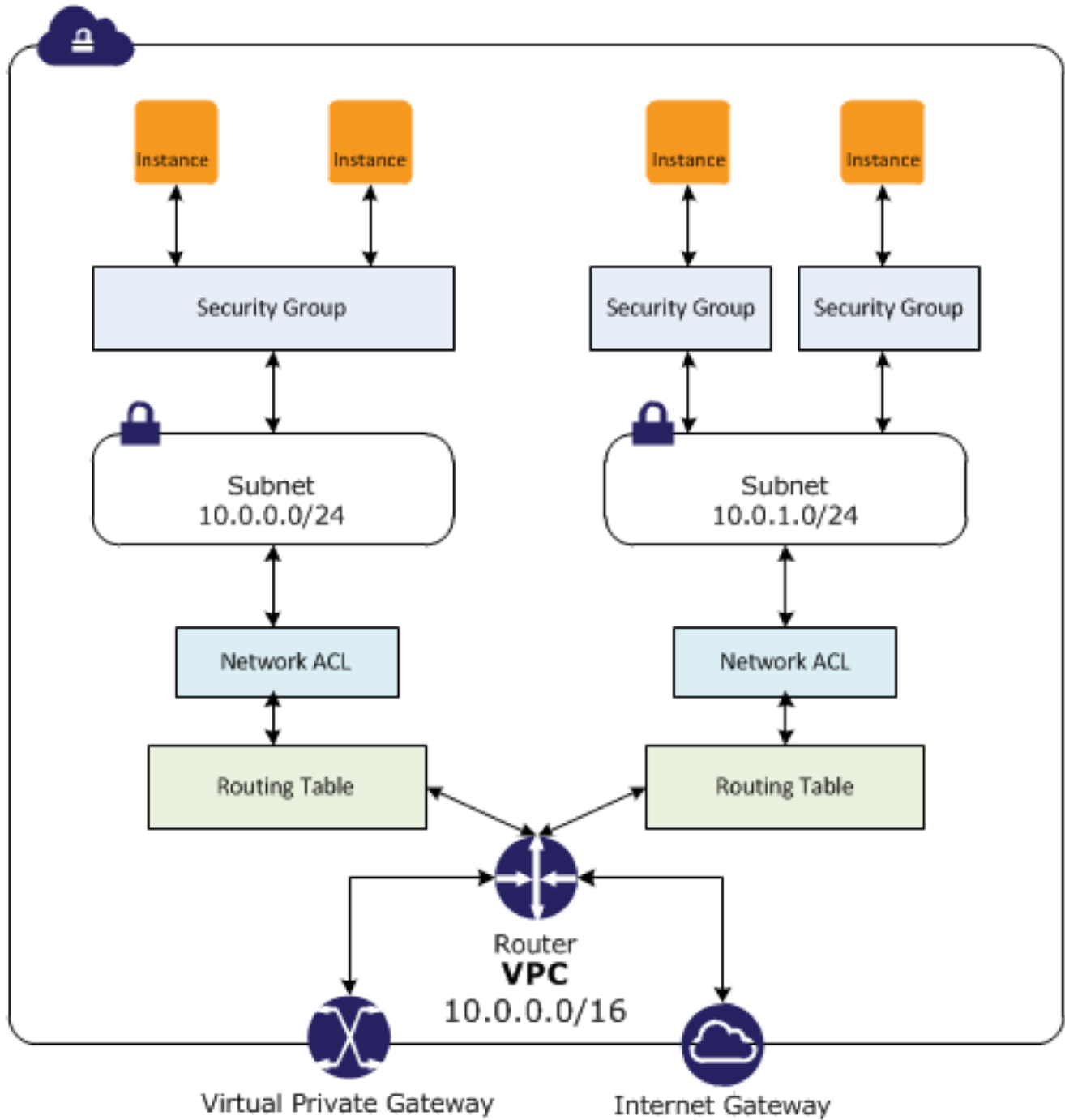
Each key pair requires a name. Be sure to choose a name that is easy to remember. Amazon EC2 associates the public key with the name that you specify as the key name. Amazon EC2 stores the public key only, and you store the private key. Anyone who possesses your private key can decrypt your login information,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

