

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

I.	Overview	5
	Amazon Virtual Private Cloud (Amazon VPC)	
	Components of Amazon VPC	
	Network Information	
II.	Basic AWS Network Setup	8
	Step 1 – Setting up your AWS account	
	Step 2 – Create a Virtual Private Cloud (VPC)	
	Step 2.1 – VPC Wizard	
III.	FortiMail Provisioning	13
	Step 3 – EC2 Launching virtual machines	
	Step 3.1 – Choosing an AMI	
	Step 3.2 – Instance type	
	Step 3.3 – Instance Details	
	Step 3.4 – Instance Storage	
	Step 3.5 – Instance Tags	
	Step 3.6 – Security groups	
	Step 3.7 – Key Pair and Launch Instance	
IV.	Network Configuration	19
	Step 4 – Configure AWS network settings	
	Step 4.1 - Associate a public “elastic” IP to the FE-VM public interface	
	Step 4.2 – Confirm the assigned Public address	
	Step 4.3 – Setting up the default route for the private network.	
	Step 4.4 – Disable Source / Destination check on the Private FortiMail interface.	
	Step 4.5 - Navigate to EC2 dash to review the Instance state	
	Step 4.6 - Access the Virtual FortiMail	
	Step 4.7 – SSH to the FortiMail unit	
V.	FortiMail Configuration	26
	Step 5.1 - Update admin password	
	Step 5.2 - Install the license	
VI.	Appendix.....	28

[Regions and Availability Zones](#)

[Amazon EC2 Key Pairs](#)

[Detailed VPC Diagram](#)

[Additional info and links](#)

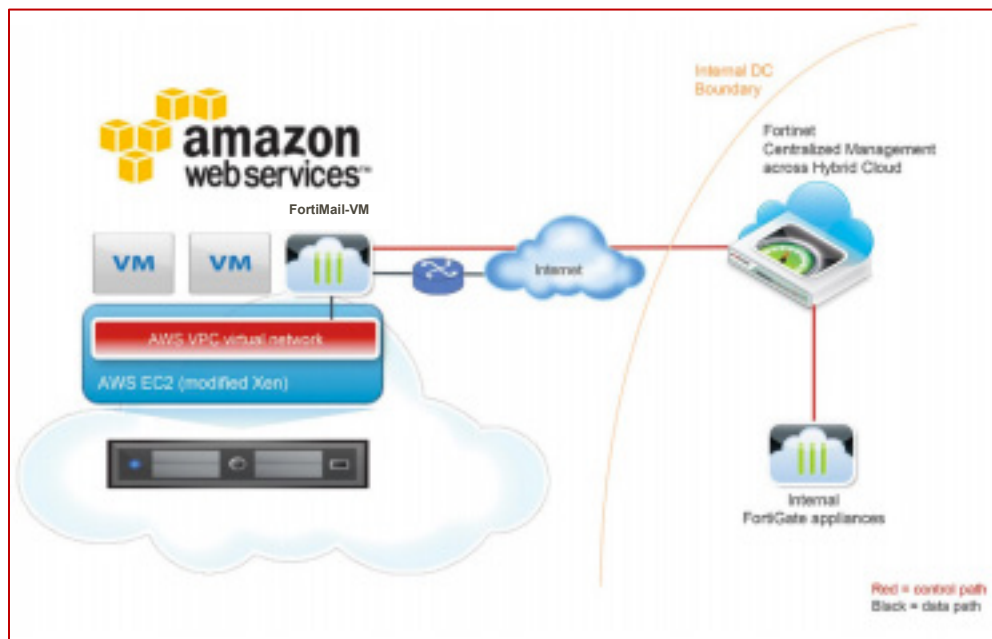
Overview

This document is design to be a quick start walk-through 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:

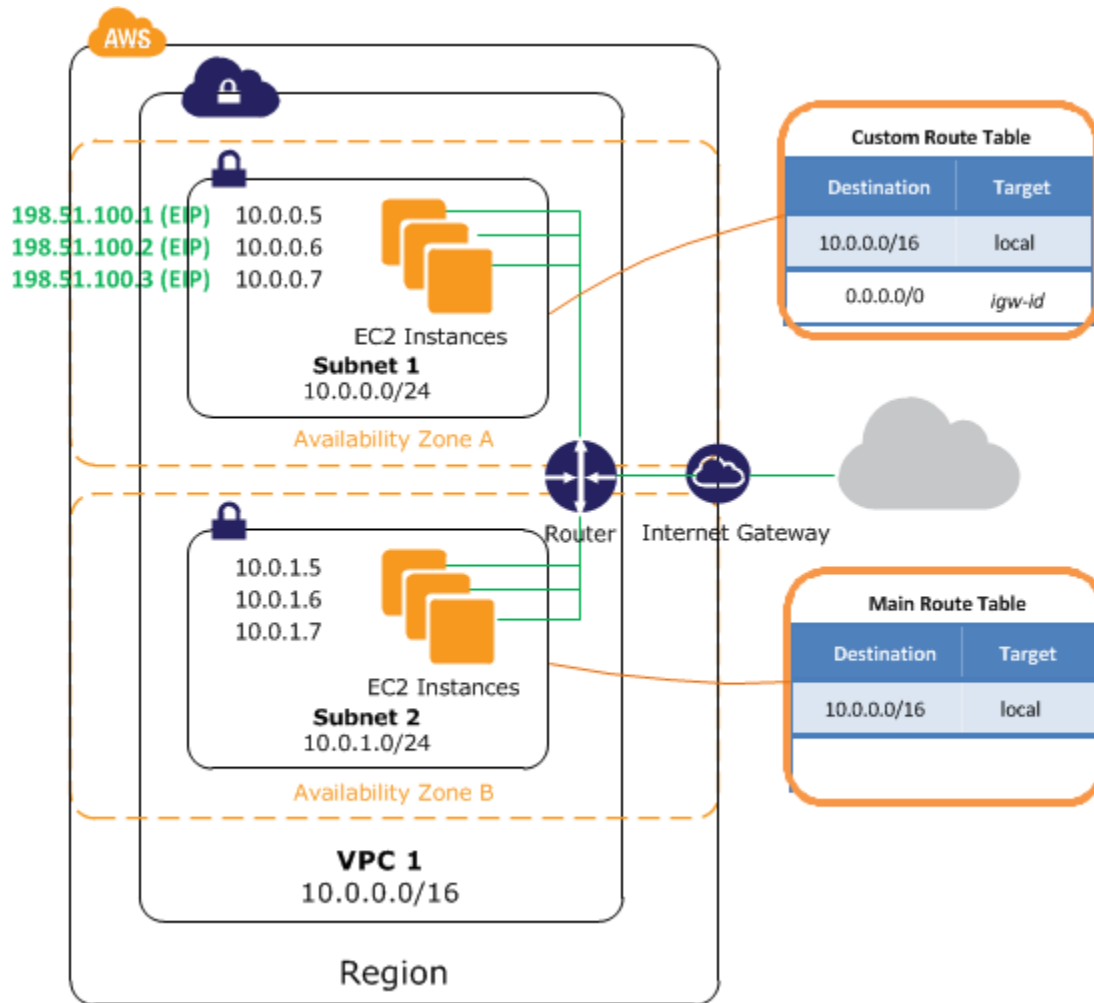
Instances without EIPs can route their traffic through a NAT instance to access the Internet. These instances use the EIP of the NAT instance to traverse the Internet. The NAT instance allows outbound communication but doesn't enable machines on the Internet to initiate a connection to the privately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

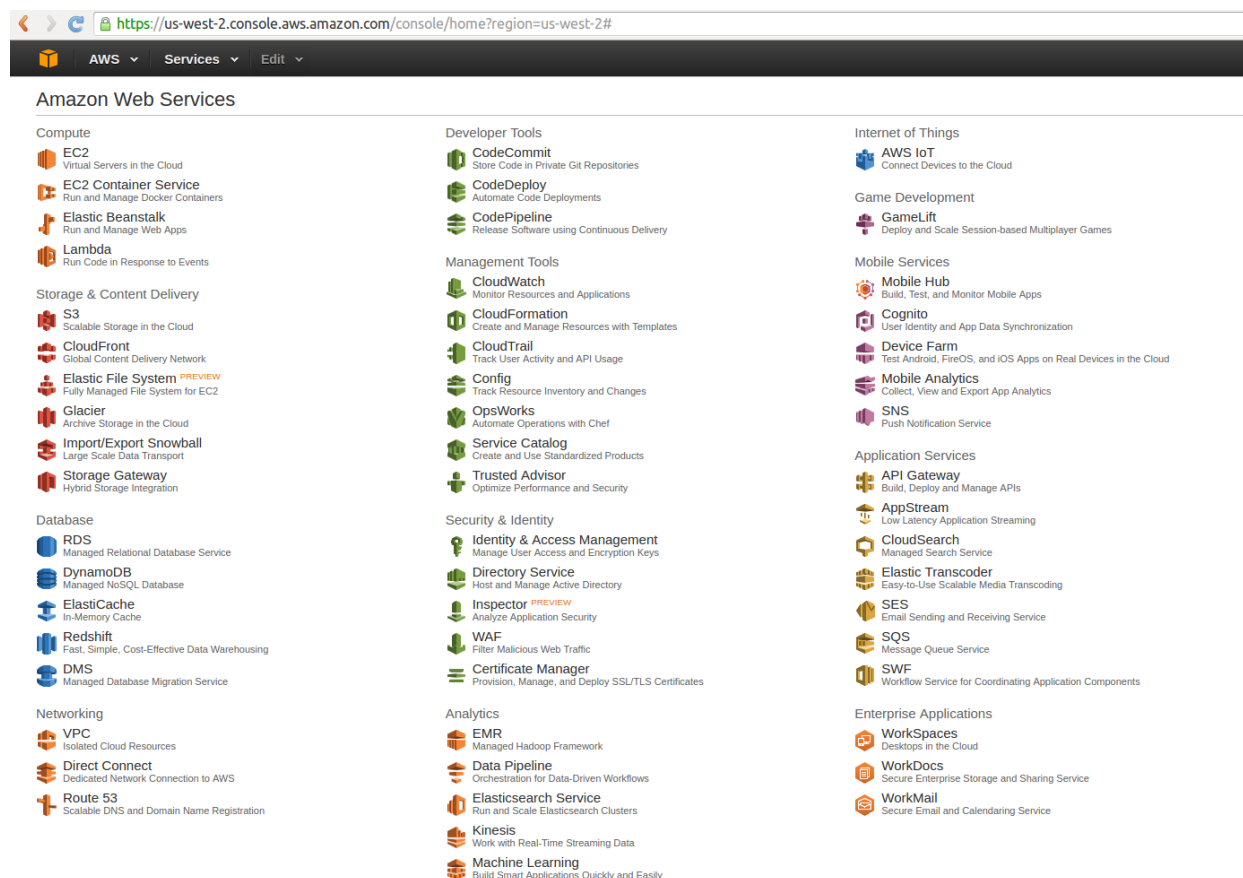
- VPC Subnet – 10.0.0.0/16
- Public Subnet - 10.0.0.0/24
- Private Subnet – 10.0.1.0/24



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.

The screenshot shows the AWS Management Console interface for the EC2 service in the US West (Oregon) region. The left sidebar contains navigation options for 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 Elastic IPs, 0 Dedicated Hosts, 0 Snapshots, 1 Volumes, 0 Load Balancers, 1 Key Pairs, and 1 Security Groups. Below this is a 'Create Instance' section with a 'Launch Instance' button and a note: 'Note: Your instances will launch in the US West (Oregon) region'. The 'Service Health' section shows 'Service Status: US West (Oregon): This service is operating normally' and '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'. The 'Scheduled Events' section shows '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.

Step 2.1 – VPC Wizard

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

The screenshot shows the AWS VPC Wizard interface in the us-west-2 region. The browser address bar displays <https://us-west-2.console.aws.amazon.com/vpc/home?region=us-west-2#wizardSelector>. The navigation bar includes the AWS logo and menu items for 'Services' and 'Edit'. The main heading is 'Step 1: Select a VPC Configuration'. On the left, a list of configuration options is shown, with 'VPC with a Single Public Subnet' selected and highlighted in blue. The description for this option states: '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.' Under the 'Creates:' section, it specifies: 'A /16 network with a /24 subnet. Public subnet instances use Elastic IPs or Public IPs to access the Internet.' A blue 'Select' button is positioned to the right of the text. To the right of the text is a diagram of the 'Amazon Virtual Private Cloud' containing a 'Public Subnet' connected to the 'Internet, S3, DynamoDB, SNS, SQS, etc.' cloud.

The screenshot shows the AWS VPC Wizard interface in the us-west-2 region. The browser address bar displays <https://us-west-2.console.aws.amazon.com/vpc/home?region=us-west-2#wizardSelector>. The navigation bar includes the AWS logo and menu items for 'Services' and 'Edit'. The main heading is 'Step 1: Select a VPC Configuration'. On the left, a list of configuration options is shown, with 'VPC with Public and Private Subnets' selected and highlighted in blue. The description for this option states: '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).' Under the 'Creates:' section, it specifies: '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.)' A blue 'Select' button is positioned to the right of the text. To the right of the text is a diagram of the 'Amazon Virtual Private Cloud' containing a 'Public Subnet' and a 'Private Subnet' connected via a 'NAT' device, both connected to the 'Internet, S3, DynamoDB, SNS, SQS, etc.' cloud.

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.

[https://us-west-2.console.aws.amazon.com/vpc/home?region=us-west-2#wizardFullpagePublicAndPrivate:](https://us-west-2.console.aws.amazon.com/vpc/home?region=us-west-2#wizardFullpagePublicAndPrivate)

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.

[https://us-west-2.console.aws.amazon.com/vpc/home?region=us-west-2#wizardFullpagePublicAndPrivate:](https://us-west-2.console.aws.amazon.com/vpc/home?region=us-west-2#wizardFullpagePublicAndPrivate)

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

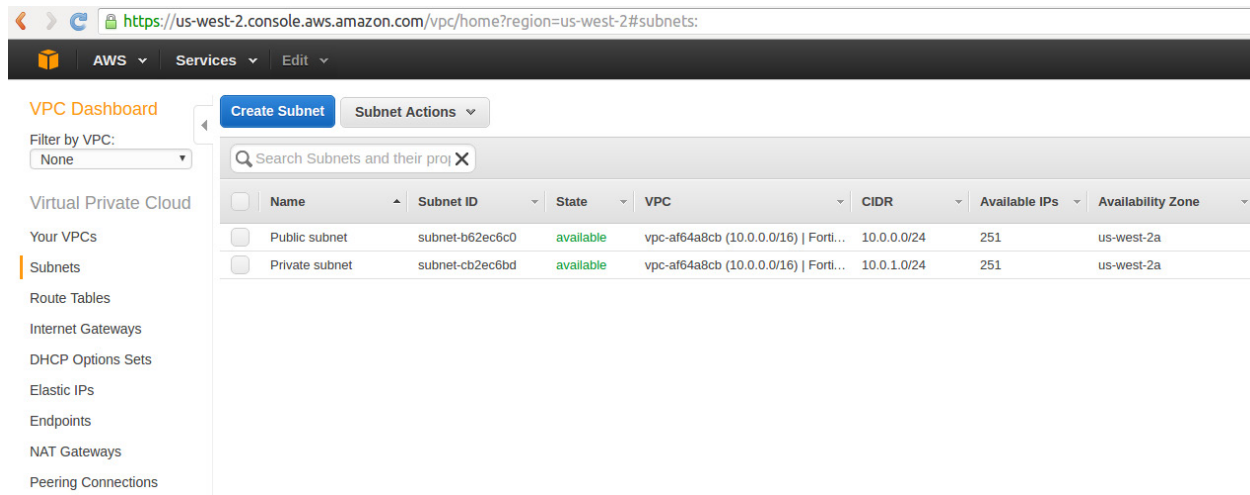
Subnet: ▼

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

52%

Running NAT Instance (This may take a few minutes)...

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



The screenshot shows the AWS VPC Dashboard in the us-west-2 region. The main content area displays a table of subnets. The table has columns for Name, Subnet ID, State, VPC, CIDR, Available IPs, and Availability Zone. Two subnets are listed: a Public subnet and a Private subnet, both in an 'available' state.

<input type="checkbox"/>	Name	Subnet ID	State	VPC	CIDR	Available IPs	Availability Zone
<input type="checkbox"/>	Public subnet	subnet-b62ec6c0	available	vpc-af64a8cb (10.0.0.0/16) Forti...	10.0.0.0/24	251	us-west-2a
<input type="checkbox"/>	Private subnet	subnet-cb2ec6bd	available	vpc-af64a8cb (10.0.0.0/16) Forti...	10.0.1.0/24	251	us-west-2a

FortiMail Provisioning

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.

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'. 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 Elastic IPs, 0 Dedicated Hosts, 0 Snapshots, 1 Volumes, 0 Load Balancers, 1 Key Pairs, and 1 Security Groups. A blue banner promotes Elastic Beanstalk. Below this is the 'Create Instance' section, which includes 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, and us-west-2c) are also operating normally. A 'Scheduled Events' section shows no events for the region.

Step 3.1 – Choosing an AMI

The screenshot shows the AWS console interface for selecting an Amazon Machine Image (AMI). The browser address bar indicates the URL: <https://us-west-2.console.aws.amazon.com/ec2/v2/home?region=us-west-2#LaunchInstanceWizard>. The navigation bar includes 'AWS', 'Services', and 'Edit'. The wizard progress bar shows seven steps: 1. Choose AMI (active), 2. Choose Instance Type, 3. Configure Instance, 4. Add Storage, 5. Tag Instance, 6. Configure Security Group, and 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-to-customize reports, ...
[More info](#)

Software Free Trial

- Free Trial (2)

Region

- Current Region (7)
- All Regions (7)

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](#)

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

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

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

Pricing Details

Bring Your Own License (BYOL)

Hourly Fees

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

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](#)

Step 3.2 – 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 (GiB)	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 <small>Free tier eligible</small>	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](#)

Step 3.3 – 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"/>	Add IP
eth1	<input type="text" value="New network interface"/>	<input type="text" value="subnet-86a571e3"/>	<input type="text" value="10.0.1.5"/>	Add IP

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

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.

The screenshot shows the 'Add Storage' step in the AWS Management Console. The breadcrumb trail includes: 1. Choose AMI, 2. Choose Instance Type, 3. Configure Instance, 4. Add Storage (highlighted), 5. Tag Instance, 6. Configure Security Group, 7. Review. The user is Justin L. Wireman. Below the breadcrumb is the heading 'Step 4: Add Storage' and a paragraph explaining that the instance will be launched with specific storage settings and that additional EBS volumes can be attached after launch. A table lists the storage configurations:

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)	60	Magnetic	N/A	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Below the table is an 'Add New Volume' button and a blue information box stating: '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.'

Step 3.5 – Instance Tags

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

The screenshot shows the 'Tag Instance' step in the AWS Management Console. The breadcrumb trail includes: 1. Choose AMI, 2. Choose Instance Type, 3. Configure Instance, 4. Add Storage, 5. Tag Instance (highlighted), 6. Configure Security Group, 7. Review. The user is Justin L. Wireman, in the Oregon region. Below the breadcrumb is the heading 'Step 5: Tag Instance' and a paragraph explaining that a tag consists of a case-sensitive key-value pair. A table lists the tags:

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

Below the table is a 'Create Tag' button with the text '(Up to 10 tags maximum)'.

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.

The screenshot shows the AWS Management Console interface for configuring a security group. The breadcrumb trail indicates the current step is '6. Configure Security Group'. The main heading is 'Step 6: Configure Security Group'. Below the heading, there is a descriptive paragraph about security groups. The 'Assign a security group' section has two radio buttons: 'Create a new security group' (selected) and 'Select an existing security group'. The 'Security group name' field contains 'PermitAll' and the 'Description' field contains 'This security group was generated by AWS Marketplace and is based on recommended setting'. Below this is a table for adding rules with columns for Type, Protocol, Port Range, and Source. A single rule is visible with Type 'All traffic', Protocol 'All', Port Range '0 - 65535', and Source 'Anywhere'. An 'Add Rule' button is present. A yellow warning box at the bottom states: '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.'

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.

The screenshot shows the 'Step 7: Review Instance Launch' screen in the AWS Management Console. A modal dialog box is open in the foreground with the title 'Select an existing key pair or create a new key pair'. The dialog contains a paragraph explaining key pairs and a note: '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.' Below the note is a dropdown menu with 'Proceed without a key pair' selected. There is a checked checkbox for 'I acknowledge that I will not be able to connect to this instance unless I already know the password built into this AMI.' and buttons for 'Cancel' and 'Launch Instances'. The background shows the 'Review Instance Launch' page with details for Instance Type (m3.medium), Security Groups, and Instance Details.

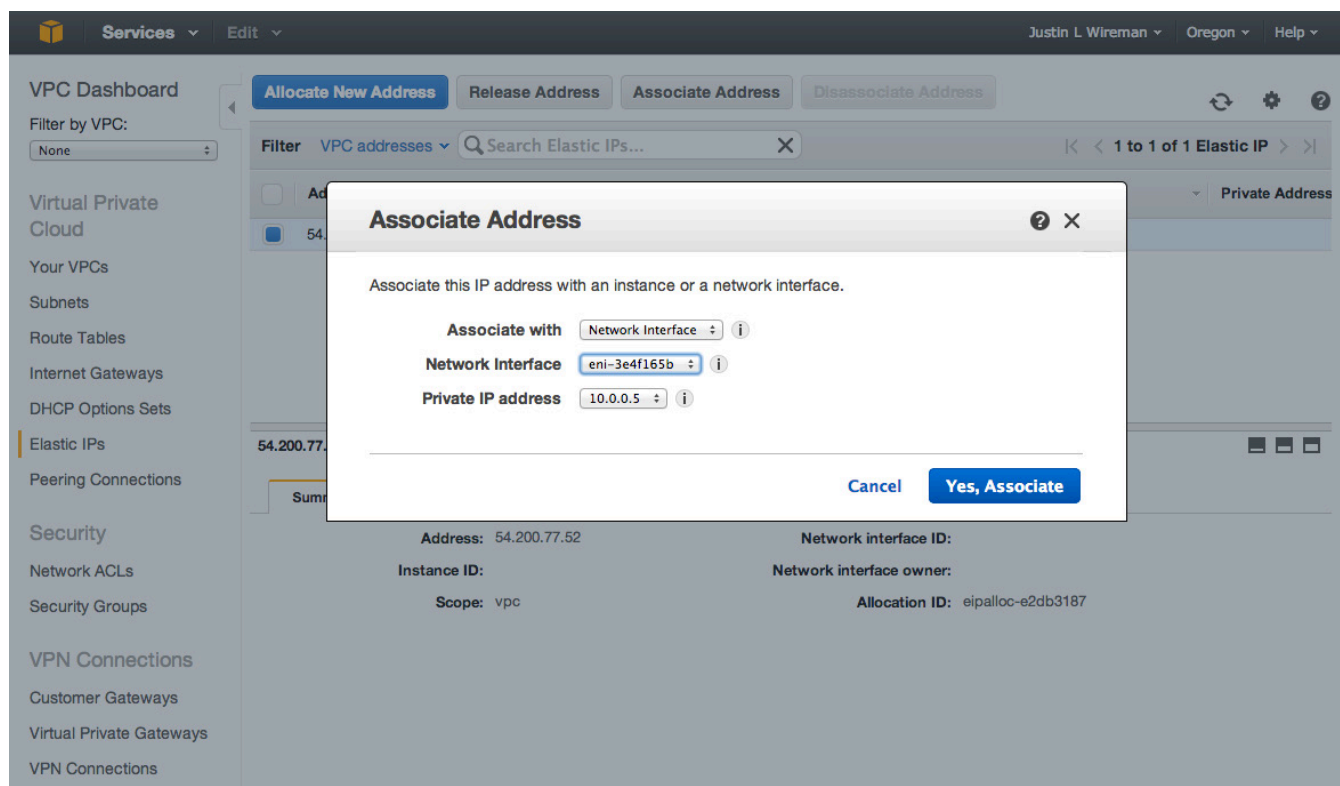
Network Configuration

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.

The screenshot shows the AWS Management Console interface for Elastic IP addresses. The left sidebar contains navigation options such as EC2 Dashboard, INSTANCES, IMAGES, ELASTIC BLOCK STORE, NETWORK & SECURITY, and AUTO SCALING. The 'Elastic IPs' option under NETWORK & SECURITY is highlighted. The main content area displays a table of Elastic IP addresses with columns for Address, Instance, Private IP Address, Scope, and Public DNS. A table below the main list provides detailed information for the selected address 54.200.77.52.

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.u

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

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.

VPC Dashboard

Filter by VPC: None

Virtual Private Cloud

Your VPCs

Subnets

Route Tables

Internet Gateways

DHCP Options Sets

Elastic IPs

Peering Connections

Security

Network ACLs

Security Groups

Create Route Table **Delete Route Table** **Set As Main Table**

Search Route Tables and their projects

Name	Route Table ID	Associated With	Main	VPC
<input type="checkbox"/>	rtb-4601c523	1 Subnet	No	vpc-0e46be6b (1)
<input checked="" type="checkbox"/>	rtb-4701c522	0 Subnets	Yes	vpc-0e46be6b (1)

rtb-4701c522

Summary **Routes** Subnet Associations Route Propagation Tags

Edit

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

rtb-4701c522

Summary **Routes** Subnet Associations Route Propagation Tags

Cancel **Save**

Destination	Target	Status	Propagated	Remove
10.0.0.0/16	local	Active	No	
0.0.0.0/0	eni-91752cf4	Active	No	✗
				✗

eni-91752cf4 | Private FG Interface
No results

Add another route

- 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

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

Services Edit

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

Create Network Interface Attach Detach Delete Actions

Filter: All VPC network interfaces Search Network Interfaces

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

Attach

Detach

Delete

Manage Private IP Addresses

Associate Address

Disassociate Address

Change Termination Behavior

Change Security Groups

Change Source/Dest. Check

Add/Edit Tags

Change Description

The screenshot shows the AWS Management Console interface for Network Interfaces. The left sidebar contains navigation options: 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), and Network Interfaces (highlighted).

The main content area displays a table of Network Interfaces with the following data:

Name	Network interface	Subnet ID	VPC ID	Zone	Security groups
Public subnet	eni-b7b094d2	subnet-c16eb9a4	vpc-663ec403	us-west-2a	PermitALL
Private FE interface	eni-b5b094d0	subnet-c66eb9a3	vpc-663ec403	us-west-2a	PermitALL
	eni-7cb69219	subnet-c16eb9a4	vpc-663ec403	us-west-2a	default

A modal dialog box titled "Change Source/Dest. Check" is open, showing the "Network Interface" as eni-b5b094d0. The "Source/dest. check" option is currently set to "Disabled" (radio button selected). The dialog includes "Cancel" and "Save" buttons.

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.

- 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 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	ec2-54-200-

Instance: **i-64fb846f** (FortiMail-VM) Elastic IP: **54.200.77.52**

[Description](#)
[Status Checks](#)
[Monitoring](#)
[Tags](#)

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-e5936f4a-0d69-479f-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

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.

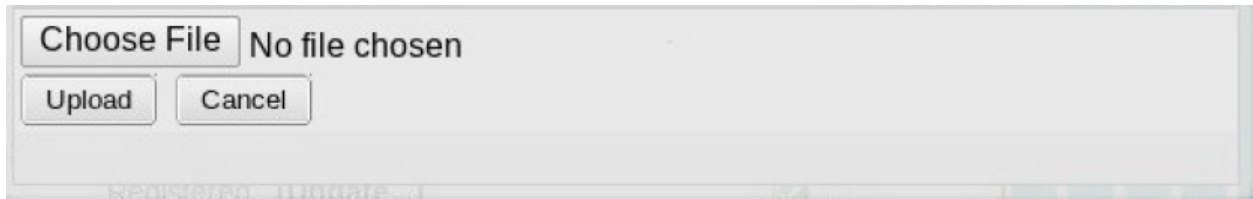
To change the admin password, go to **System > Administrator**. Edit the admin user and set up the password. By default, the admin user does not have a password.

The screenshot displays the FortiMail configuration interface. On the left is a vertical navigation menu with categories: Monitor, Maintenance, System (highlighted), Network, Configuration, Customization, Administrator (highlighted), High Availability, Certificate, Encryption, Mail Settings, User, Policy, Data Loss Prevention, Profile, AntiSpam, AntiVirus, Email Archiving, and Log and Report. The main content area is titled 'Administrator' and 'Access Profile'. The 'Administrator' tab is active, showing the 'Edit Administrator' form. The form includes the following fields and controls:

- Enable:** A checked checkbox.
- Administrator:** A text input field containing 'admin'.
- Domain:** A dropdown menu showing '--System--'.
- Access profile:** A dropdown menu showing 'super_admin_prof', with 'New...' and 'Edit...' buttons to its right.
- Authentication type:** A dropdown menu showing 'Local'.
- Change password:** A checkbox with a downward arrow, currently unchecked.
- Old password:** An empty text input field.
- New password:** An empty text input field.
- Confirm password:** An empty text input field.
- Trusted hosts:** Two rows of input fields. The first row contains '0.0.0.0' and '0'. The second row contains '::' and '0'. There are '+' and '-' icons to the right of the second row.
- Language:** A dropdown menu showing 'English'.
- Theme:** A dropdown menu showing 'Red Grey', with a 'Use Current' button to its right.
- Buttons:** 'OK' and 'Cancel' buttons are located at the bottom left of the form area.

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.

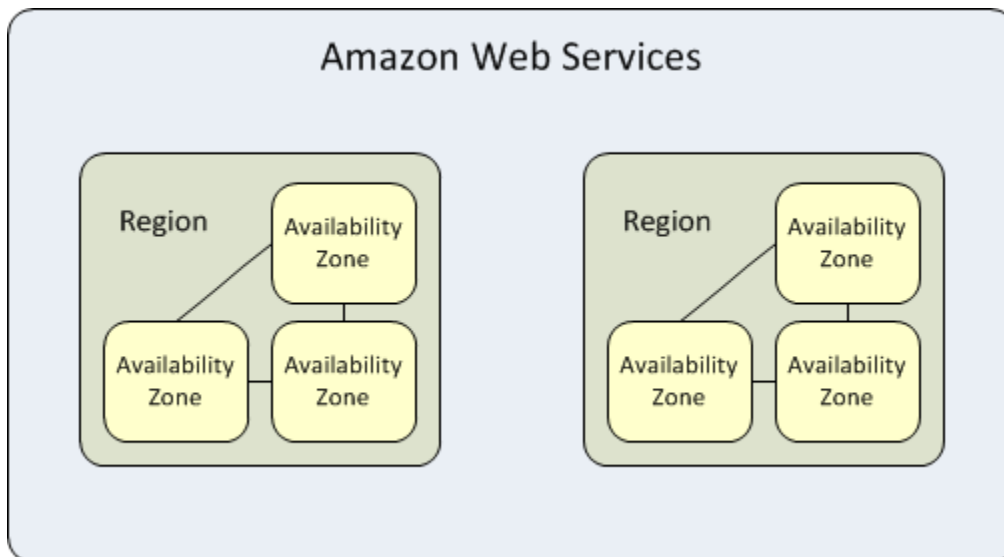


Appendix

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](#).

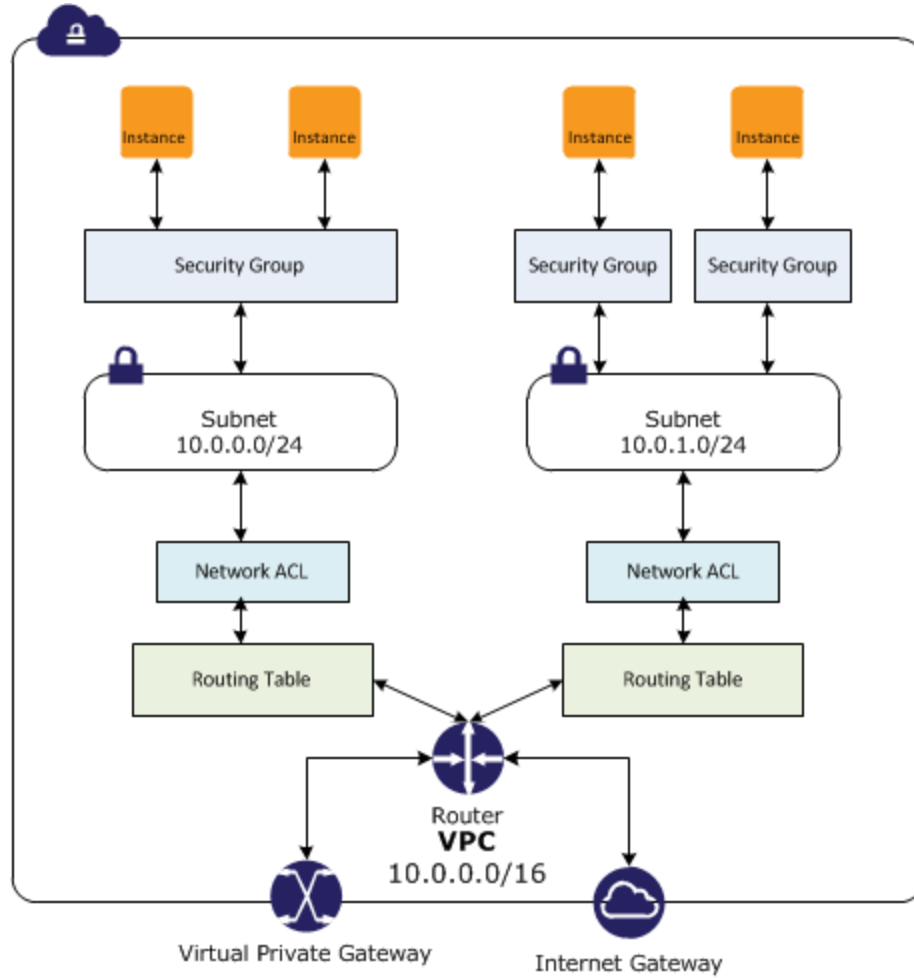
Each key pair requires a name. Be sure to choose a name that is easy to remember. Amazon EC2 associates the public key with the name that you specify as the key name. Amazon EC2 stores the public key only, and you store the private key. Anyone who possesses your private key can decrypt your login information,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



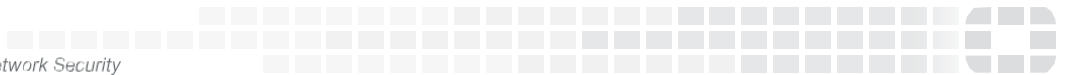
Additional info and links

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

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



High Performance Network Security



Copyright© 2015 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. In no event does Fortinet make any commitment related to future deliverables, features, or development, and circumstances may change such that any forward-looking statements herein are not accurate. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.