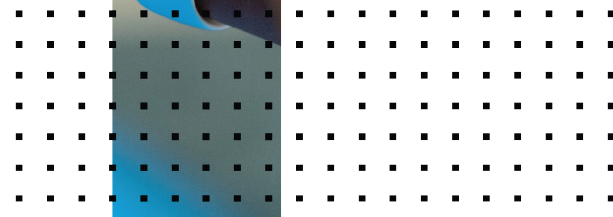
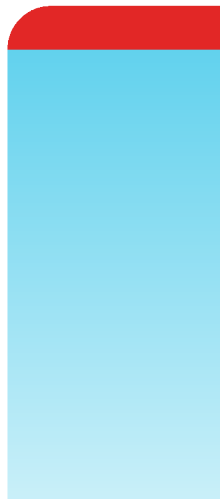


Cloud Deployment Guide (AWS EC2)

FortiProxy 7.0



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



April 18, 2024

FortiProxy 7.0 Cloud Deployment Guide (AWS EC2)

45-700-674629-20240418

TABLE OF CONTENTS

Change Log	4
Overview	5
Before deploying the FortiProxy VM	6
Deploying the FortiProxy VM	11

Change Log

Date	Change Description
2022-04-15	Initial release.

Overview

Amazon Elastic Compute Cloud (Amazon EC2) provides scalable computing capacity in the Amazon Web Services (AWS) cloud. Using Amazon EC2 eliminates your need to invest in hardware up front, so you can develop and deploy applications faster. You can use Amazon EC2 to launch virtual servers, configure security and networking, and manage storage.

The following sections explain how to deploy the FortiProxy VM on AWS EC2.

Before deploying the FortiProxy VM

1. Create a Virtual Private Cloud (VPC) and specify the IPv4 address range for your VPC.

The screenshot shows the AWS console interface for creating a VPC. The top navigation bar includes the AWS logo, 'Services', 'Resource Groups', a search icon, a notification bell, the user email 'blau@fortinet.com', and the region 'Ohio'. Below the navigation bar, the breadcrumb 'VPCs > Create VPC' is visible. The main heading is 'Create VPC'. A descriptive paragraph explains that a VPC is an isolated portion of the AWS cloud and that an IPv4 address range must be specified as a CIDR block. The form contains the following fields:

- Name tag:** A text input field containing 'FortiProxy-VPC'.
- IPv4 CIDR block*:** A text input field containing '10.1.0.0/16'.
- IPv6 CIDR block:** A radio button selection with two options: 'No IPv6 CIDR Block' (selected) and 'Amazon provided IPv6 CIDR block'.
- Tenancy:** A dropdown menu set to 'Default'.

At the bottom of the form, there is a legend for '* Required', a 'Cancel' button, and a blue 'Create' button.

2. Create the subnet and specify your subnet's IP address block.

Subnets > Create subnet

Create subnet

Specify your subnet's IP address block in CIDR format; for example, 10.0.0.0/24. IPv4 block sizes must be between a /16 netmask and /28 netmask, and can be the same size as your VPC. An IPv6 CIDR block must be a /64 CIDR block.

Name tag

VPC*

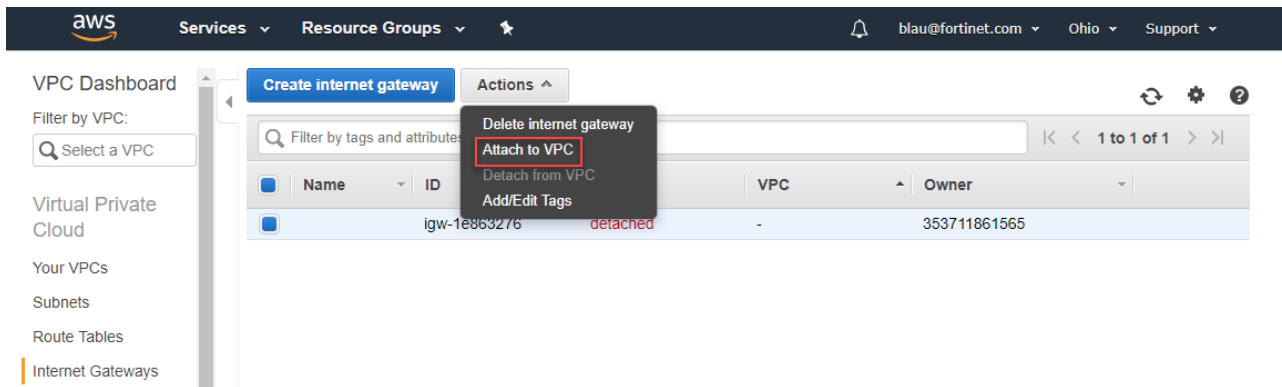
VPC CIDRs	CIDR	Status	Status Reason
	10.1.0.0/16	associated	

Availability Zone

IPv4 CIDR block*

* Required Cancel **Create**

3. Create an Internet gateway and attach it to your VPC.



4. Create or use the default route table and configure the subnet associations according to the actual network.

Before deploying the FortiProxy VM

The screenshot shows the AWS Management Console interface for the 'Route Tables' section. The left sidebar contains navigation options like 'Virtual Private Cloud', 'Your VPCs', 'Subnets', 'Route Tables', etc. The main content area displays a list of route tables. The 'FortiProxy-VPC-Route-Table' is selected. Below the list, the 'Routes' tab is active, showing a table of routes for the selected route table.

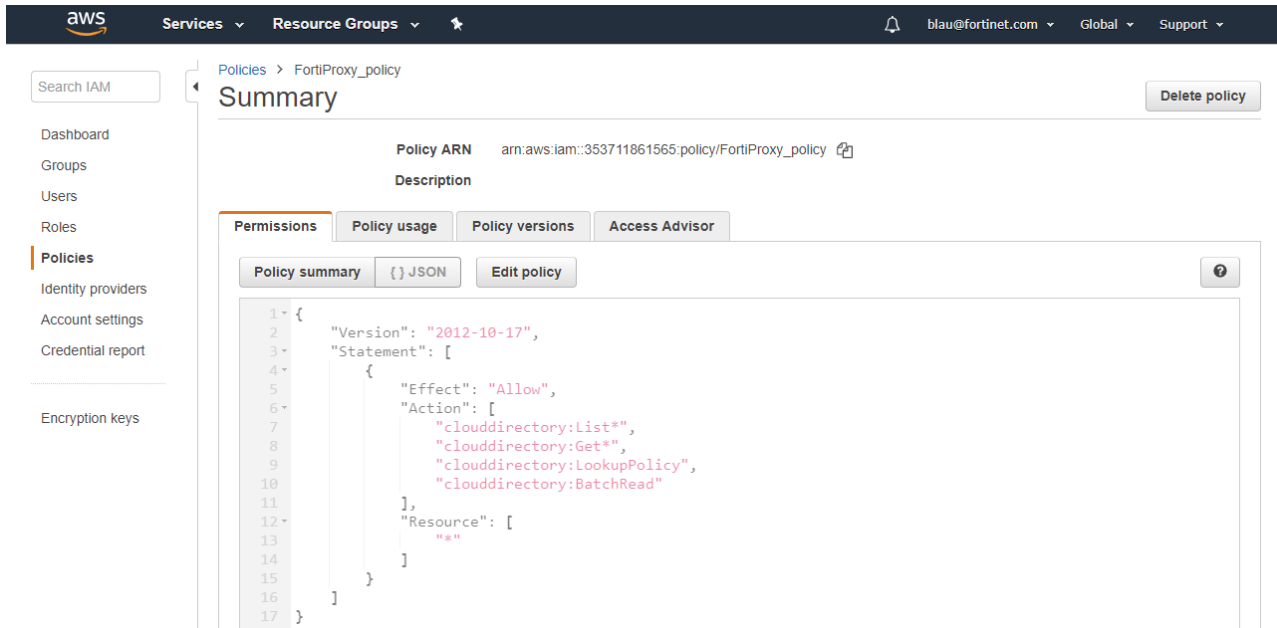
Destination	Target	Status	Propagated
10.1.0.0/16	local	active	No
0.0.0.0/0	igw-1e863276	active	No

5. Create a security group and configure the inbound rules and outbound rules.

The screenshot shows the AWS Management Console interface for the 'Security Groups' section. The left sidebar contains navigation options like 'Virtual Private Cloud', 'Your VPCs', 'Subnets', 'Route Tables', etc. The main content area displays a list of security groups. The 'Security_Group_Allow_All' is selected. Below the list, the 'Inbound Rules' tab is active, showing a table of inbound rules for the selected security group.

Type	Protocol	Port Range	Source	Description
All TCP	TCP	0 - 65535	0.0.0.0/0	

6. Create the IAM policy.



The following is an example of an AWS permissions policy:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "elasticbeanstalk:*",
        "ec2:*",
        "elasticloadbalancing:*",
        "sns:*",
        "sqs:*",
        "rds:*",
        "iam:*"
      ],
      "Resource": "*"
    }
  ]
}
```

7. Create a role and attach the permissions policies.

Create role



Review

Provide the required information below and review this role before you create it.

Role name*

Use alphanumeric and '+=, @-_' characters. Maximum 64 characters.

Role description

Maximum 1000 characters. Use alphanumeric and '+=, @-_' characters.

Trusted entities AWS service: ec2.amazonaws.com

Policies [FortiProxy_policy](#)

Permissions boundary Permissions boundary is not set

No tags were added.

* Required

[Cancel](#)

[Previous](#)

[Create role](#)

Deploying the FortiProxy VM

After creating a Virtual Private Cloud (VPC), you are ready to deploy the FortiProxy VM on Amazon Web Services' Elastic Compute Cloud (Amazon EC2).

1. Log in to AWS and ensure that you have a VPC (Virtual Private Cloud).
2. Go to EC2 and select *Launch Instance*.

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

Step 1: Choose an Amazon Machine Image (AMI) Cancel and Exit

An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. You can select an AMI provided by AWS, our user community, or the AWS Marketplace; or you can select one of your own AMIs.

Q Search for an AMI by entering a search term e.g. "Windows" X

Quick Start 1 to 38 of 38 AMIs >

- My AMIs**
- AWS Marketplace**
- Community AMIs
- Free tier only

	Amazon Linux 2 AMI (HVM), SSD Volume Type - ami-02cbb802e03574ba (64-bit x86) / ami-06a134062219ad132 (64-bit Arm)	Select
	Amazon Linux 2 comes with five years support. It provides Linux kernel 4.14 tuned for optimal performance on Amazon EC2, systemd 219, GCC 7.3, Glibc 2.26, Binutils 2.29.1, and the latest software packages through extras.	64-bit (x86) 64-bit (Arm)
	Amazon Linux AMI 2018.03.0 (HVM), SSD Volume Type - ami-0cd3dfa4e37921605	Select
	The Amazon Linux AMI is an EBS-backed, AWS-supported image. The default image includes AWS command line tools, Python, Ruby, Perl, and Java. The repositories include Docker, PHP, MySQL, PostgreSQL, and other packages.	64-bit (x86)
	Red Hat Enterprise Linux 7.6 (HVM), SSD Volume Type - ami-0b500ef59d5335eee (64-bit x86) / ami-0302c1ecc74930ba5 (64-bit Arm)	Select
	Red Hat Enterprise Linux version 7.6 (HVM), EBS General Purpose (SSD) Volume Type	64-bit (x86) 64-bit (Arm)
	SUSE Linux Enterprise Server 15 (HVM), SSD Volume Type - ami-0eb9f56db22854f8f (64-bit x86) / ami-064a69af9b77fa05 (64-bit Arm)	Select
	SUSE Linux Enterprise Server 15 (HVM), EBS General Purpose (SSD) Volume Type. Public Cloud, Advanced Systems Management, Web and Scripting, and Legacy modules enabled.	64-bit (x86) 64-bit (Arm)
	Ubuntu Server 18.04 LTS (HVM), SSD Volume Type - ami-0c55b159cbf9afe1f0 (64-bit x86) / ami-0f2057f28f0a44d06 (64-bit Arm)	Select
	Ubuntu Server 18.04 LTS (HVM), EBS General Purpose (SSD) Volume Type. Support available from Canonical (http://www.ubuntu.com/cloud/services).	64-bit (x86) 64-bit (Arm)

Are you launching a database instance? Try Amazon RDS. Hide

Amazon Relational Database Service (RDS) makes it easy to set up, operate, and scale your database on AWS by automating time-consuming database management tasks. With RDS, you can easily deploy Amazon Aurora, MariaDB, MySQL, Oracle, PostgreSQL, and SQL Server databases on AWS. Aurora is a MySQL- and PostgreSQL-compatible, enterprise-class database at 1/10th the cost of commercial databases. [Learn more about RDS](#)

[Launch a database using RDS](#)

3. Select *AWS Marketplace*.

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

Step 1: Choose an Amazon Machine Image (AMI) Cancel and Exit

An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. You can select an AMI provided by AWS, our user community, or the AWS Marketplace; or you can select one of your own AMIs.

Q Search for an AMI by entering a search term e.g. "Windows" X

Quick Start 1 to 38 of 38 AMIs >

- My AMIs**
- AWS Marketplace**
- Community AMIs
- Free tier only

	Amazon Linux 2 AMI (HVM), SSD Volume Type - ami-02cbb802e03574ba (64-bit x86) / ami-06a134062219ad132 (64-bit Arm)	Select
	Amazon Linux 2 comes with five years support. It provides Linux kernel 4.14 tuned for optimal performance on Amazon EC2, systemd 219, GCC 7.3, Glibc 2.26, Binutils 2.29.1, and the latest software packages through extras.	64-bit (x86) 64-bit (Arm)
	Amazon Linux AMI 2018.03.0 (HVM), SSD Volume Type - ami-0cd3dfa4e37921605	Select
	The Amazon Linux AMI is an EBS-backed, AWS-supported image. The default image includes AWS command line tools, Python, Ruby, Perl, and Java. The repositories include Docker, PHP, MySQL, PostgreSQL, and other packages.	64-bit (x86) 64-bit (Arm)

4. Enter *FortiProxy* and press *Enter* to find the Fortinet FortiProxy-VM Security Web Gateway (BYOL).

Deploying the FortiProxy VM

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

Step 1: Choose an Amazon Machine Image (AMI) Cancel and Exit

An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. You can select an AMI provided by AWS, our user community, or the AWS Marketplace, or you can select one of your own AMIs.

Q FortiProxy

Quick Start (0) 1 to 1 of 1 Products

My AMIs (0)

AWS Marketplace (1)

Community AMIs (1)

Categories

All Categories

Infrastructure Software (1)

Operating System

Clear Filter

All Linux/Unix

FORTINET Fortinet FortiProxy-VM Security Web Gateway (BYOL)

★★★★★ (0) | FortiProxy 1.1.1 | By Fortinet, Inc.

Bring Your Own License + AWS usage fees

Linux/Unix, Other 1.1.1 | 64-bit (x86) Amazon Machine Image (AMI) | Updated: 4/10/19

FortiProxy is a secure web proxy that protects employees against Internet-borne attacks by incorporating multiple detection techniques such as web filtering, DNS filtering, data ...

[More info](#)

The following results for "FortiProxy" were found in other catalogs:

1 results in Community AMIs

Community AMIs are AMIs that are shared by the general AWS community

Select

5. Select the Fortinet FortiProxy-VM Security Web Gateway (BYOL).

Fortinet FortiProxy-VM Security Web Gateway (BYOL)

FORTINET

Fortinet FortiProxy-VM Security Web Gateway (BYOL)

FortiProxy is a secure web proxy that protects employees against Internet-borne attacks by incorporating multiple detection techniques such as web filtering, DNS filtering, data loss prevention, antivirus, intrusion prevention, and advanced threat protection. It helps enterprises enforce internet compliance using granular application control. ...

[More info](#)

[View Additional Details in AWS Marketplace](#)

Pricing Details

Bring Your Own License (BYOL)

Hourly Fees

Instance Type	Software	EC2	Total
m5.large	\$0.00	\$0.096	\$0.096/hr
m5.xlarge	\$0.00	\$0.192	\$0.192/hr
m5.2xlarge	\$0.00	\$0.384	\$0.384/hr
m5.4xlarge	\$0.00	\$0.768	\$0.768/hr
c5.large	\$0.00	\$0.085	\$0.085/hr
c5.xlarge	\$0.00	\$0.17	\$0.17/hr
c5.2xlarge	\$0.00	\$0.34	\$0.34/hr
c5.4xlarge	\$0.00	\$0.68	\$0.68/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.

Product Details

By Fortinet, Inc.

Customer Rating ★★★★★ (0)

Latest Version FortiProxy 1.1.1

Base Operating System Linux/Unix, Other 1.1.1

Delivery Method 64-bit (x86) Amazon Machine Image (AMI)

License Agreement [End User License Agreement](#)

On Marketplace Since 4/10/19

AWS Services Required Amazon EC2, VPC

Highlights

- Security - Advanced Threat Protection against any Internet-borne attacks
- Performance - Improving user QoE with advanced content caching, video stream splitting and WAN optimization.

Cancel Continue

6. Select *Continue*.

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

Step 2: Choose an Instance Type

Instance Type	Instance Class	VCpus	Memory (GiB)	Storage	Network	Accelerated Networking
<input type="radio"/>	Compute optimized	c5d.9xlarge	36	72	1 x 900 (SSD)	Yes
<input type="radio"/>	Compute optimized	c5d.18xlarge	72	144	2 x 900 (SSD)	Yes
<input checked="" type="radio"/>	Compute optimized	c5.large	2	4	EBS only	Yes
<input type="radio"/>	Compute optimized	c5.xlarge	4	8	EBS only	Yes
<input type="radio"/>	Compute optimized	c5.2xlarge	8	16	EBS only	Yes

7. Select one of the instance types and then select *Review and Launch*.

Boot from General Purpose (SSD) ✕

General Purpose (SSD) volumes provide the ability to burst to 3000 IOPS per volume, independent of volume size, to meet the performance needs of most applications and also deliver a consistent baseline of 3 IOPS/GiB.

- Make General Purpose (SSD) the default boot volume for all instance launches from the console going forward (recommended).
- Make General Purpose (SSD) the boot volume for this instance.
- Continue with Magnetic as the boot volume for this instance.

Free tier eligible customers can get up to 30GB of General Purpose (SSD) storage.

8. Select *Make General Purpose (SSD) the boot volume for this instance* and then select *Next*.

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

Step 7: Review Instance Launch

Please review your instance launch details. You can go back to edit changes for each section. Click **Launch** to assign a key pair to your instance and complete the launch process.

⚠️ Your instance configuration is not eligible for the free usage tier
 To launch an instance that's eligible for the free usage tier, check your AMI selection, instance type, configuration options, or storage devices. [Learn more about free usage tier eligibility and usage restrictions.](#)

[Don't show me this again](#)

AMI Details [Edit AMI](#)

Fortinet FortiProxy-VM Security Web Gateway (BYOL)
 FortiProxy-VM64-AWS build0154 v1.1.1_GA
 Root Device Type: ebs Virtualization type: hvm

Hourly Software Fees: \$0.00 per hour on c5.large instance. Additional taxes or fees may apply. Software charges will begin once you launch this AMI and continue until you terminate the instance.

By launching this product, you will be subscribed to this software and agree that your use of this software is subject to the pricing terms and the seller's [End User License Agreement](#)

Instance Type [Edit instance type](#)

Instance Type	ECUs	vCPUs	Memory (GiB)	Instance Storage (GB)	EBS-Optimized Available	Network Performance
c5.large	8	2	4	EBS only	Yes	Up to 10 Gigabit

Security Groups [Edit security groups](#)

Security group name Fortinet FortiProxy-VM Security Web Gateway -BYOL--FortiProxy 1-1-1-AutogenByAWSMP-
Description This security group was generated by AWS Marketplace and is based on recommended settings for Fortinet FortiProxy-VM Security Web Gateway (BYOL) version FortiProxy 1.1.1 provided by Fortinet, Inc.

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

9. Select **Launch**.
10. Select **Create a new key pair**, enter a name for the key pair, and then select **Download Key Pair**.

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.](#)

Create a new key pair

Key pair name

FortiProxyKeyPair

Download Key Pair


💬 You have to download the private key file (*.pem file) before you can continue. Store it in a secure and accessible location. You will not be able to download the file again after it's created.


[Cancel](#) [Launch Instances](#)

11. Select **Launch Instances**.

Deploying the FortiProxy VM

Launch Status

 **Your instances are now launching**
The following instance launches have been initiated: [i-0e9080e4186bac00a](#) [View launch log](#)

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

How to connect to your instances

Your instances are launching, and it may take a few minutes until they are in the **running** state, when they will be ready for you to use. Usage hours on your new instances will start immediately and continue to accrue until you stop or terminate your instances. Click **View Instances** to monitor your instances' status. Once your instances are in the **running** state, you can connect to them from the Instances screen. [Find out how to connect to your instances.](#)

Getting started with your software

To get started with Fortinet FortiProxy-VM Security Web Gateway (BYOL) To manage your software subscription

[View Usage Instructions](#) [Open Your Software on AWS Marketplace](#)

Here are some helpful resources to get you started

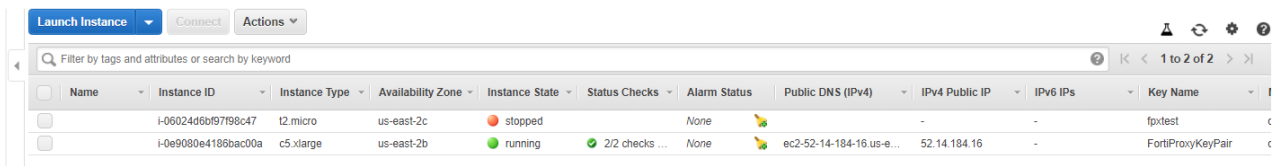
- How to connect to your Linux Instance
- Learn about AWS Free Usage Tier
- Amazon EC2: User Guide
- Amazon EC2: Discussion Forum

While your instances are launching you can also

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

[View Instances](#)

12. Select *View Instances*.



The screenshot shows the AWS Management Console 'Instances' page. At the top, there are buttons for 'Launch Instance', 'Connect', and 'Actions'. Below is a search bar and a table of instances. The table has columns for Name, Instance ID, Instance Type, Availability Zone, Instance State, Status Checks, Alarm Status, Public DNS (IPv4), IPv4 Public IP, IPv6 IPs, and Key Name. Two instances are visible: one in a 'stopped' state and one in a 'running' state.

Name	Instance ID	Instance Type	Availability Zone	Instance State	Status Checks	Alarm Status	Public DNS (IPv4)	IPv4 Public IP	IPv6 IPs	Key Name
	i-06024d6bf97f98c47	t2.micro	us-east-2c	stopped		None				fpctest
	i-0e9080e4186bac00a	c5.xlarge	us-east-2b	running	2/2 checks ...	None	ec2-52-14-184-16.us-e...	52.14.184.16		FortiProxyKeyPair



www.fortinet.com

Copyright© 2024 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., 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 Chief Legal Officer, 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. 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.