# TABLE OF CONTENTS

I. Overview .................................................................................................................. 4
   Introduction .................................................................................................................. 4
   What is FortiSandbox ................................................................................................... 4
   FortiSandbox on AWS Use Cases ................................................................................. 4

II. Basic AWS Network Setup ......................................................................................... 6
   Step 1. Create a virtual private cloud (VPC) .............................................................. 6
   Step 1.2 Create the subnet for FSA Firmware ............................................................. 7
   Step 1.3 Create Internet gateway ............................................................................... 9

III. FortiSandbox Provisioning ......................................................................................... 11
   Step 2 EC2 Launching FSA virtual instance ............................................................... 11
   Step 2.1 Choose an Amazon Machine Image (AMI) ..................................................... 11
   Step 2.2 Choose an instance type .............................................................................. 12
   Step 2.3 Configure instance details .......................................................................... 12
   Step 2.4 Add storage ................................................................................................. 13
   Step 2.5 Add tags ...................................................................................................... 13
   Step 2.6 Configure security group ............................................................................. 14
   Step 2.7 Review instance launch ................................................................................ 14

IV. Network Configuration .............................................................................................. 17
   Step 3 Configure FSA network settings ...................................................................... 17
   Step 3.1 Assigning elastic IP to instance .................................................................... 17
   Step 3.2 FortiSandbox web GUI access ..................................................................... 17
   Step 3.3 DNS configuration ....................................................................................... 19
   Step 3.4 Access FortiSandbox CLI (SSH) .................................................................. 19

V. FortiSandbox Testing ................................................................................................. 20
   FortiSandbox dashboard and contract information ......................................................... 20
   On-Demand submit test using remote VM ...................................................................... 21

VI. Advanced AWS Setup for Using VMs ...................................................................... 23
   Step 4 Setup an AWS account for FortiSandbox .......................................................... 23
   Step 4.1 Create IAM group and user ........................................................................... 23
Step 4.2 Attach policy ................................................................. 25
Step 4.3. Create IAM users and the AWS API key ........................................ 30
Step 4.4. FSA GUI AWS configuration ................................................... 33
Step 5 Prepare VM subnet for FortiSandbox ............................................... 34
Step 5.1 Create the private subnet .......................................................... 35
Step 5.2 Create NAT gateway and set route table ....................................... 35
Step 5.3 Create and attach DHCP options to VPC ..................................... 38

VII. Option A: Install Trial VM .......................................................... 40
Install trial VM via CLI ................................................................. 40
Configure trial VM clones on web GUI ............................................... 41
Submit on-demand test .................................................................. 42

VIII. Option B: Install Custom VMs ........................................................... 46
Guidelines to prepare a custom VM image ........................................... 46
Install custom VM via CLI .............................................................. 46
Submit on-demand test .................................................................. 47
I. OVERVIEW

INTRODUCTION

Fortinet’s FortiSandbox on AWS enables organizations to defend against advanced threats natively in the cloud working alongside network, email, endpoint, and other security, or as an extension to their on-premises security architectures to leverage scale with complete control.

FortiSandbox Amazon Machine Image is available via AWS Marketplace and this documentation provides users with an easy-to-follow, step-by-step guide for a successful deployment of FortiSandbox.

FortiSandbox on AWS can be installed as standalone zero-day threat prevention or work in conjunction with your existing FortiGate, FortiMail, or FortiWeb AWS instances to identify malicious and suspicious files, ransomware, and network threats.

WHAT IS FORTISANDBOX

FortiSandbox uses a two-stage process to identify zero-day, advanced malware including ransomware, and generate relevant threat intelligence.

Stage 1: Pre-filtering is performed by an engine powered by Fortinet’s threat research and FortiGuard Labs Intelligence.

Stage 2: Dynamic behavior analysis is performed on objects to determine if they are malicious. Rating verdicts are returned to the originating device in real-time to act upon, natively within Fortinet Fabric security products, third-party vendor security products via JSON API, or as a feed via STIX format.

FORTISANDBOX ON AWS USE CASES

Use Case #1: Instantaneous Indicators of Compromise (IOC) Intelligence Sharing Across Multi-Clouds

In hybrid or multi-cloud environments, it’s critical to get first-hand IOC intelligence for zero-day malware protection. FortiSandbox instantly shares session information and IOC related to the malware behavior. If there are multiple FortiSandbox instances (physical, virtualized, or cloud) present, you can identify the synchronization rule for the intelligence update.

Use Case #2: Fabric-Based Deep Analysis for Zero-Day Malware Detection

FortiSandbox on AWS introduces elasticity for on-demand sandbox resources when they are needed, which can be very costly in the traditional on-premises setting. When working with other Fortinet products like FortiGate, FortiWeb, or FortiMail, it shares intelligence for faster, automated response to threats.

FortiSandbox continues to be a powerful use case for public cloud when no prior malware signature exists. When the firewall does not find the AV malicious profile in the HTTP or web traffic, it submits and queues up the file sample in FortiSandbox on AWS for in-depth analysis until the verdict is reached.

ADAPTIVE NOTIFICATION AND REMEDIATION

The intelligence is shared across the Fortinet Security Fabric. Every signature and IOC that FortiSandbox generates is automatically propagated across all FortiGate firewalls and FortiClient endpoints for immediate blocking or quarantine actions to avoid further damage.
When anticipated traffic is down it can release the AWS compute resources if not needed.

**Use Case #3: FortiSandbox Cloud Scan Automation**

Amazon Elastic File System (Amazon EFS) provides simple, scalable file storage for use with Amazon EC2 instances in the AWS Cloud. As EFS is used often in cloud migration such as dataset migration, on-demand backup, or cloud bursting scenarios, you can mount your Amazon EFS file systems on your on-premises data center servers when connected to your Amazon VPC with AWS Direct Connect or through a FortiGate site-to-site secured connection. In the process, you can insert FortiSandbox on premises or in AWS. Or you can perform malware analysis in the EFS-to-EFS backup solution to ensure clean file backup.
The other way to use FortiSandbox through NFS mount is to leverage AWS Storage Gateway. By mounting a file share and mapping it to an Amazon S3 bucket using AWS Storage Gateway, you can configure AWS S3 as the NFS or SMB network share for FortiSandbox malware analysis. When used in conjunction with the Amazon S3 event notification feature, it enables you to receive notifications when certain file events happen in the bucket and use the AWS Lambda function to queue the file sample to FortiSandbox for malware analysis.

Other use cases such as preventing malware penetration in a closed / isolated network can be considered. Without any external malware signatures, FortiSandbox can help perform zero-day malware analysis instead. For more architecture discussion, please email aws@fortinet.com if you need to clarify the use cases.

II. BASIC AWS NETWORK SETUP

STEP 1. CREATE A VIRTUAL PRIVATE CLOUD (VPC)

Navigate to VPC Dashboard > Your VPCs > Create VPC. There’s a default VPC but you should always create a new VPC.
DEPLOYMENT GUIDE: FORTISANDBOX ON AWS

- Click **Create VPC** to get the Create VPC window. Provide any name in **Name tag**, e.g., FortiSandbox, to be isolated from your current works.
- Enter IPv4 CIDR block as 10.0.0.0/16 to ease scale-out issues in the future.
- Click **No IPv6 CIDR Block**.
- Select **Tenancy** as Default and click on **Yes, Create**.

You can view the created VPC (FortiSandbox) below.

**STEP 1.2 CREATE THE SUBNET FOR FSA FIRMWARE**

We need to create two subnets for FortiSandbox.

- Public subnet with IPv4 CIDR 10.0.0.0/24, which is connected to the FSA-VM management interface.
- Private subnet with IPv4 CIDR 10.0.1.0/24, which is connected to all VM clones and FSA-VM.

**Note**

You can skip creating a private subnet if you don’t use “Trial VMs” or “Custom VMs.”

Without a private subnet, you can still use Remote VM for file analysis.

To create a subnet, click **Subnets** and **Create Subnet**. You will get the Create Subnet window. Type any name for **Name tag**. Select the created VPC under VPC, and give the IPv4 CIDR block as 10.0.0.0/24 (for public subnet). Then click on **Yes, Create**.
Again, click Create Subnet to get a Create Subnet window. Give any name for Name tag, select your created VPC under VPC, give the IPv4 CIDR block as 10.0.0.0/24 (for private subnet), then click on Yes, Create.

We can view the created public and private subnets as below. Step 1.3 Create Internet gateway
STEP 1.3 CREATE INTERNET GATEWAY

Under Virtual Private Cloud, select Internet Gateways and click on Create Internet Gateway. Give any name for Name tag and click Yes, Create.

Once the Internet Gateway is created, click Attach to VPC then select your created VPC. Click Yes, Attach.
Once we are attached to VPC we can view the state as attached, as shown below.

Under Virtual Private Cloud select Route Tables then click Create Route Table for public subnet.

It will show the Create Route Table window. Give any name for Name tag, select the created VPC under VPC, then click Yes, Create.
Go to **Subnet Associations**, click **Edit**, check the public subnet, then click **Save**.

![Subnet Associations](image)

Go to **Routes**, click **Add another route**, give Destination as 0.0.0.0/0 and under **Target** select your created Internet Gateway for public subnet. Then click **Save**.

![Routes](image)

### III. FORTISANDBOX PROVISIONING

#### STEP 2 EC2 LAUNCHING FSA VIRTUAL INSTANCE

#### STEP 2.1 CHOOSE AN AMAZON MACHINE IMAGE (AMI)

At Search FortiSandbox on the [AWS Marketplace](https://aws.amazon.com), choose a FortiSandbox Amazon Machine Image `FSAAWS.310 ami-f06d9a88` or the latest AMI link after your bring-your-own-license (BYOL) purchase.
STEP 2.2 CHOOSE AN INSTANCE TYPE

Select `t2.medium` for balanced burstable performance, and click **Next: Configure Instance Details**.

STEP 2.3 CONFIGURE INSTANCE DETAILS

Configure the instance details:
- **Number of instances**: 1
- **Purchasing option**: N/A
- **Network**: select your created FortiSandbox VPC
- **Subnet**: select your created public subnet
- **Auto-assign Public IP**: Disable
- **IAM role**: None
- **Shutdown behavior**: Stop
- **Enable termination protection**: N/A
- **Monitoring**: N/A
- **Tenancy**: Shared - Run a shared hardware instance
- **eth0**: select your created public subnet, Auto assign (or any IP in that subnet)
- Then click Add device
- **eth1**: select your created private subnet, Auto assign (or any IP in that subnet)

**Note:**
You can skip adding **eth1** if you don’t use “Trial VMs” or “Custom VMs.” But you can always add it back when the instance is at “stopped” status.
STEP 2.4 ADD STORAGE

Click Add New Volume. Make sure the device column has the right values reflecting /dev/sdb and then enter **32 GB** in the Size column. Check the “Delete on Termination” boxes for both volumes, then click Next: Add Tags.

STEP 2.5 ADD TAGS

Leave it untouched and click Next: Configure Security Group.
**STEP 2.6 CONFIGURE SECURITY GROUP**

Click create a new security group, give any name for security group name and provide a suitable description for Description.

Type > All traffic  
Protocol > All  
The Port Range will come up automatically once you choose All under protocol  
Source > select Custom from dropdown. Give the SourceIP as 0.0.0.0/0  
Then click Review and Launch.

**STEP 2.7 REVIEW INSTANCE LAUNCH**

Review the page and then click on Launch

You will get a pop-up box as below to create a new key pair from the dropdown. Choose Create a new key pair and give a key pair name. Then Download and save the private key file, then click on Launch Instances.  
You can import an existing public key for remote access to the running instance.
After launching the instance, the below screen shows the FortiSandbox instance up and running. Click **View Instances** to view instance state.

It takes few minutes to change the state checks from initializing to 2/2 checks.

Once the instance is in running state, go to that created instance and give it any name.
Select the created instance then click on **Actions>Instance Settings>Get Instance Screenshot** to view the status of the launched instance.
IV. NETWORK CONFIGURATION

STEP 3 CONFIGURE FSA NETWORK SETTINGS

STEP 3.1 ASSIGNING ELASTIC IP TO INSTANCE

Create a new Elastic IP (EIP) if there isn’t one to allocate under Virtual Private Cloud. Click Elastic IPs, then Allocate new address.

Click Allocate to get the new EIP address.

Once you see the new Elastic IP address, click Close.

STEP 3.2 FORTISANDBOX WEB GUI ACCESS

Copy the IPv4 Public IP from the created instance.
Paste the copied IP address in a new browser window to log in to the FortiSandbox Web GUI.

- **Default username:** admin
- **Default password:** give your created instance ID. (You can find it on the EC2 Management Console)

Once logged in you can view the UI as below
**STEP 3.3 DNS CONFIGURATION**

Navigate to Network, select System DNS, and update the columns with respective details under DNS Configuration. Then click OK.

- **Primary DNS Server** – 8.8.4.4
- **Secondary DNS Server** – 8.8.8.8

**STEP 3.4 ACCESS FORTISANDBOX CLI (SSH)**

The FortiSandbox has CLI commands that are accessed when accessing the FortiSandbox via console or by using an SSH or TELNET client.

Log in to CLI using the Elastic IP of your created instance by giving the username as admin and with ppk file. Please note: If you don’t choose the without key pair option, log in using password `<InstanceID>`.

Before login, convert the saved pem file which you downloaded while creating the key pair to ppk file.

Run the following commands to interact with FortiSandbox using CLI

**NOTE:** The below commands are for illustration purposes only. You can use relevant commands per the requirement.
V. FORTISANDBOX TESTING

FORTISANDBOX DASHBOARD AND CONTRACT INFORMATION

Note: VM License is not needed for AWS FortiSandbox.

Note: To get future firmware updates we can contact Fortinet support site http://support.fortinet.com
ON-DEMAND SUBMIT TEST USING REMOTE VM

Navigate to Scan Input > File On-Demand > Submit File. You will get a dialog box.

Click on choose file and upload the file fiddler2setup.exe, and submit. You should get a “CLEAN” rating after you send the file to FortiSandbox if the uploaded file is clean and not harmful.

Click on Browse and upload the file then click on Submit.
After uploading file, you can view **File On-Demand** and select any file to check.

Click the view file icon under **Action**.

You can see the file check details as shown below.
VI. ADVANCED AWS SETUP FOR USING VMS

STEP 4 SETUP AN AWS ACCOUNT FOR FORTISANDBOX

There are a few account preparations required before you launch the FortiSandbox in the AWS Marketplace.

STEP 4.1 CREATE IAM GROUP AND USER

To create one or more IAM users from the AWS Management Console, please follow the step-by-step instructions below.

Log in to the AWS console with your credentials.

Once you log in to the console, click Search, type IAM
You can view the IAM dashboard as below.

Click on Groups to create a new group.

After clicking Create New Group, set the group name created earlier in IAM management, by entering any name, for example, QA_FortiSandboxTest.
**STEP 4.2 ATTACH POLICY**

Please make sure that you have the right permissions to attach policies to a group. Below are the policies that need to be added to the group we have created above (QA_FortiSandbox).

Attach the following policy names:

- AmazonEC2FullAccess
- AWSConfigUserAccess
- IAMUserChangePassword
- IAMUserSSHKeys
- PowerUserAccess
- IAMFullAccess

Click **Filter**, type **AmazonEC2FullAccess**, check the box as shown below.

![AmazonEC2FullAccess](image1)

Click **Filter**, type **AWSConfigUserAccess**, check the box as shown below.

![AWSConfigUserAccess](image2)

Click **Filter**, type **IAMUserChangePassword**, check the box as shown below.

![IAMUserChangePassword](image3)
Click Filter, type IAMUserSSHKeys, check the box as shown below.

Click Filter, type IAMFullAccess, check the box as shown below.

Click Filter, type PowerUserAccess, check the box as shown below.

Click Create Group after Review.
After clicking **Create Group**, you can see the created group as below.

Check the **QA_FortiSandboxTest** to view the summary of the group.

Once you check the **QA_FortiSandboxTest**, you can view as below.
Once you check the QA_FortiSandboxTest, you can view as below.

Under Permissions you can view the attached policies you’ve added and under Inline Policies click on Click here.

Select Custom Policy. We use the policy editor to customize our own set of permissions.
DEPLOYMENT GUIDE: FORTISANDBOX ON AWS

Give the policy name and the policy code, then click Validate Policy. If validation succeeds, click Apply Policy {

"Version": "2012-10-17",
"Statement": [

  "Effect": "Allow",
  "Action": [
    "iam:CreateRole",
    "iam:PutRolePolicy",
    "iam:ListRoles"
  ],
  "Resource": [
    "*"
  ]
]

Now you can view created policy names under Inline Policies.
**STEP 4.3. CREATE IAM USERS AND THE AWS API KEY**

Click **Add user** to create a user.

Provide the user name and check **AWS Management Console access**. At **Console password**, check **Custom password** and click **Next Permissions**.

Search and check the Group Name you created and click **Next Review**.
Once you’ve added the group, click **Create user.**

After adding the user to the group, you can click on **Groups** to view the created user.
After adding a user, sign out from AWS console and sign in with the created user

![AWS Console](image-url)

Give the created user log in credentials and reset your password. Click Confirm password change.

![Password Change](image-url)

**AWS API KEY**

API Gateway supports multiple mechanisms of access control, including metering or tracking API uses by clients using API keys.

To create AWS API key navigate to IAM>Users>tester1>security credentials>create access key.

![Create Access Key](image-url)
Once you click on the create access key button, you will get a pop-up. Click on Download.csv file to save the access key ID and secret access key to a CSV file on your computer. After you have downloaded the CSV file, choose Close.

**STEP 4.4. FSA GUI AWS CONFIGURATION**

Navigate to System > AWS Config, and fill in the required AWS API key information with the setup wizard. Give the private IP address name in Private Subnet then click Configuration Wizard.

Select Region as us-west-2 from the dropdown and click Next.
Give your created **VPC ID** and click **Next**.

Provide your created **Security Group ID** and click **Save**.

Once you see the configuration is successfully saved, click **Close**.

**STEP 5 PREPARE VM SUBNET FOR FORTISANDBOX**

**STEP 5.1 CREATE THE PRIVATE SUBNET**

Private subnet with IPv4 CIDR 10.0.1.0/24, which is connected to all VM clones and FSA-VM

Click **Create Subnet** to get a Create Subnet window. Give any name for **Name tag**, select your created VPC under VPC, give the IPv4 CIDR block as 10.0.1.0/24 (for private subnet), then click on **Yes, Create**
We can view the created private subnets as below.

**STEP 5.2 CREATE NAT GATEWAY AND SET ROUTE TABLE**

Under **Virtual Private Cloud** select **NAT Gateways**. Click **Create NAT Gateway**.
Select the created public subnet

From the dropdown for **Subnet** and select the created Elastic IP. Click **Create a NAT Gateway.**

![Create NAT Gateway](image)

**NOTE**

- NAT/Internet Gateway for Private subnet is not recommended by AWS security team, and should be temporary for testing and not running real malware
- AWS security recommends using AWS VPN or AWS Direct Connect to route out of an egress point to any third-party Internet provider

Once the NAT Gateway is created, it will show the created NAT Gateway as below

![NAT Gateway](image)

Under **Virtual Private Cloud** select **Route Tables** then click **Create Route Table** for public subnet.

![Create Route Table](image)
It will show the Create Route Table window. Give any name for Name tag, select the created VPC under VPC, then click Yes, Create.

Go to Subnet Associations, click Edit, check the public subnet, then click Save.

Go to Routes, click Add another route, give Destination as 0.0.0.0/0 and under Target select your created Internet Gateway for public subnet. Then click Save.
Go to Subnet Associations, click Edit, check the created private subnet, and click Save.

Go to Routes, click Add another route, give Destination as 0.0.0.0/0, and under Target select your created NAT Gateway for private subnet, then click Save.

STEP 5.3 CREATE AND ATTACH DHCP OPTIONS TO VPC

Under Virtual Private cloud select DHCP Options Sets. Click create DHCP Options Sets and give any name for Name tag.

Domain name servers: 10.0.1.229 [give the primary IP you gave while creating the eth1. If auto-assigned, take the IP from instance details.] Then click on Yes, Create.
Go back to Your VPCs. Right click your created VPC entry and select Edit DHCP Options Set.

Choose the created DHCP options set and Save.
VII. OPTION A: INSTALL TRIAL VM

INSTALL TRIAL VM VIA CLI

Log in to CLI using the Elastic IP of your created instance by giving the username as admin and with ppk file. Please note: If you don’t choose the without key pair option, log in using password `<InstanceID>`.

Before login, convert the saved pem file which you downloaded while creating the key pair to ppk file.

Run the status command to view the status of the VM.

Run installvms, and you should be able to see and config the VM images clones on GUI.
DEPLOYMENT GUIDE: FORTISANDBOX ON AWS

CONFIGURE TRIAL VM CLONES ON WEB GUI

After installation in CLI go to Fortisandbox Web GUI > Virtual Machine > VM Images. You can view installed VMs. If you want to change count under Clone click Edit and Apply.

After Apply, you can see the launched instance in the AWS console. If you give the Clone count as 4, you can view four instances.
DEPLOYMENT GUIDE: FORTISANDBOX ON AWS

SUBMIT ON-DEMAND TEST

Navigate to Scan Input > File On-Demand > Submit File. You will get a dialog box.

Click on choose file and upload the file fiddler2setup.exe, and submit. You should get a “CLEAN” rating after you send the file to FortiSandbox if the uploaded file is clean and not harmful.

The file fsa_dropper.vxe, is a fake high-risk sample created by Fortinet. FortiSandbox will detect harmful malicious behavior as High Risk. Similarly, upload any file that might be harmful, e.g., fsa_dropper.vxe. Click on Submit, then you will be alerted by FortiSandbox that this file is harmful if it contains any malware.
After uploading files, you can view **File On-Demand** and select any file to check.

Click the view file icon under **Action**.

You can see the clean file check details below.
Similarly, click on the view file icon of your submitted file for risk analysis.

Click on the file as shown below.

You will get a page like this. Click on Details.
The High-Risk Dropper page is below.
VIII. OPTION B: INSTALL CUSTOM VMS

GUIDELINES TO PREPARE A CUSTOM VM IMAGE

Use a custom VM on FortiSandbox AWS. FortiSandbox AWS supports custom VMs. The user can provide the VHD image for a created customer VM, and FSA firmware can load the VM image and use it for sample analysis.

- Create the VHD image with a virtualization software solution, e.g., VirtualBox
- Please refer to the custom VM section in FortiSandbox 2.5.0 Administration Guide for details

Key guidelines:
- When creating the VM, specify VHD as the disk image format.
- The disk controller must be IDE.
- The disk size must not be over 20 GB.
- The OS must have the PV Driver installed. (current ver, 7.4.6) https://s3.amazonaws.com/ec2-downloads-windows/Drivers/AWSPVDriverSetup.zip
- Copy the FortiSandbox Tools folder to any location (e.g., C:\) of the custom VM, and add the “FSALauncher.exe” to be an auto-startup program. (Use the Startup Folder or Task Scheduler).
- Windows should have been configured to auto login.

Share the VHD file from SSH/FTP from a public server, or an internal server that can be accessed from the FSA firmware.

INSTALL CUSTOM VM VIA CLI

Go to FSA firmware CLI.

- Import the VHD image using CLI command “vm-customized”
  - E.g., vm-customized -cn -tscp -s52.43.149.247 -uroot -pf0rtinet123 -f/win7x64.vhd -voWindows7_64 -vnCustomWIN7x64 -k9610847d5f6def21fa1f72867a072f
  - E.g., vm-customized -cn -tscp -s35.167.136.225 -uroot -pf0rtinet123 -f/Win10X64AWS.vhd -voWindows10_64 -vnCustomWIN10x64 -ke23f3a58e6d097357f129cdae89d00f9
- (Please refer to help when you use “vm-customized” on CLI.)
SUBMIT ON-DEMAND TEST

Navigate to Scan Input > File On-Demand > Submit File. You will get a dialog box.

Click on choose file and upload the file fiddler2setup.exe, and submit. You should get a “CLEAN” rating after you send the file to FortiSandbox if the uploaded file is clean and not harmful.

The file fsa_dropper.vxe, is a fake high-risk sample created by Fortinet. FortiSandbox will detect harmful malicious behavior as High Risk. Similarly, upload any file that might be harmful, e.g., fsa_dropper.vxe. Click on Submit, then you will be alerted by FortiSandbox that this file is harmful if it contains any malware.
After uploading files, you can view **File On-Demand** and select any file to check.

Click the view file icon under **Action**.

You can see the clean file check details below.
Similarly, click on the view file icon of your submitted file for risk analysis.

Click on the file as shown below.

You will get a page like this. Click on Details.
The High-Risk Dropper page is below.