FORTINET
High Performance Network Security

FortiOS™ Handbook - Sandbox Inspection

VERSION 5.6.3

FORTIOS 5.6 VERSION

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

http://cookbook.fortinet.com/how-to-work-with-fortinet-support/

FORTIGATE COOKBOOK

http://cookbook.fortinet.com

FORTINET TRAINING SERVICES

http://www.fortinet.com/training

FORTIGUARD CENTER

http://www.fortiguard.com

FORTICAST

http://forticast.fortinet.com

END USER LICENSE AGREEMENT

http://www.fortinet.com/doc/legal/EULA.pdf

FORTINET PRIVACY POLICY

https://www.fortinet.com/corporate/about-us/privacy.html

FEEDBACK

Email: techdocs@fortinet.com

1/24/2018

FortiOS™ Handbook - Sandbox Inspection

TABLE OF CONTENTS

Change Log **4**
Introduction **5**
What's new in FortiOS 5.6 ..... **6**
FortiOS 5.6.1 6
New file extension lists for determining which file types to send to FortiSandbox (379326) 6
FortiSandbox integration with AntiVirus in quick mode (436380) 6
An Overview of Sandbox Inspection **7**
What is Sandbox Inspection? 7
FortiSandbox Appliance vs FortiSandbox Cloud 7
Sending Files for Sandbox Inspection 8
Using FortiSandbox with a FortiGate **10**
Connecting a FortiGate to FortiSandbox 10
FortiSandbox Console 11
Sandbox Integration **12**
Overview 12
AntiVirus 12
Web Filtering 12
FortiClient Profiles 13
Example Configuration 13
Sandbox Inspection FAQ **16**

Change Log

Date	Change Description
January 18, 2018	Clarifications throughout the document.
November 29, 2017	Corrected error in table in FortiSandbox Appliance vs FortiSandbox Cloud
August 15, 2017	Edit to reflect FortiOS 5.6.1 and to add information on support for the monitoring of files in different protocols.
March 30, 2017	Initial FortiOS 5.6 release.

Introduction

This guide explains how to set up sandbox inspection using FortiSandbox with a FortiGate. It contains the following sections:

- What's New in FortiOS 5.6.1: Highlights new features added.
- An Overview of Sandbox Inspection: General information about how sandbox inspection works.
- Using FortiSandbox with a FortiGate: How to set up sandbox inspection on a FortiGate.
- Sandbox Integration: Integrating sandbox inspection with FortiGate, FortiSandbox, and FortiClient.
- Sandbox Inspection FAQ: Frequently asked questions to help troubleshoot sandbox inspection.

What's new in FortiOS 5.6

The following section describes new Sandbox Integration features added to FortiOS 5.6.1.

FortiOS 5.6.1

These features first appeared in FortiOS 5.6.1.

New file extension lists for determining which file types to send to FortiSandbox (379326)

This feature introduces two new file extension lists:

- File extensions to submit to FortiSandbox even though the AV engine says they are unsupported.
- File extensions to exclude from submitting to FortiSandbox even though the AV engine says they are supported.

These lists are configured on the FortiSandbox, not the FortiGate, and are dynamically loaded on the FortiGate via quarantine.

These lists are only file extensions and not file types detected by the AV engine using magic bytes. Pattern matching is done on the extension of the filename only.

Syntax

```
diag sys scanunit reload-fsa-ext
```

FortiSandbox integration with AntiVirus in quick mode (436380)

FortiSandbox options in an AntiVirus Security Profile in quick scanning mode can now be enabled with CLI commands.

CLI syntax

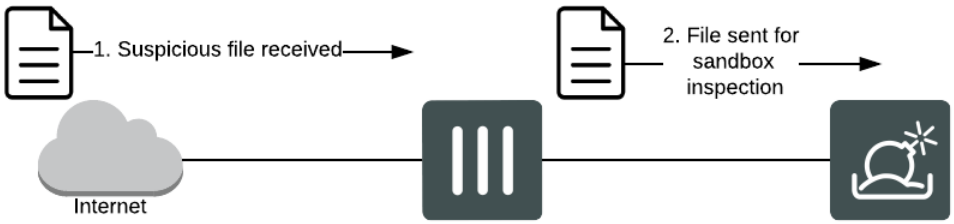
```
config antivirus profile
   edit default
      set ftgd-analytics disable/everything
      set analytics-max-upload 10
      set analytics-wl-filetype 0
      set analytics-bl-filetype 0
      set analytics-db enable/disable
      set scan-mode quick
   end
```

An Overview of Sandbox Inspection

This section contains information about how Fortinet sandbox inspection works.

- What is Sandbox Inspection?
- FortiSandbox Appliance vs FortiSandbox Cloud
- Sending Files for Sandbox Inspection

What is Sandbox Inspection?



Sandbox inspection is a network process that allows files to be sent to a separate device, such as FortiSandbox, to be inspected without risking network security. This allows the detection of threats which may bypass other security measures, including zero-day threats.

You can configure your FortiGate device to send suspicious files to FortiSandbox for inspection and analysis. The FortiGate queries scan results and retrieves scan details. The FortiGate can also download malware packages as a complimentary AV signature database to block future appearances of the same malware and download URL packages as complimentary web filtering black list.

When a FortiGate sends files for sandbox inspection, the FortiSandbox uses virtual machines (VMs) running different operating systems to test the file and to determine if it is malicious. If the file exhibits risky behavior, or is found to contain a virus, a new signature can be added to the FortiGuard AntiVirus signature database.

When a FortiGate learns from FortiSandbox that a terminal is infected, the administrator can push instruction for self-quarantine on a registered FortiClient host.

FortiSandbox can process multiple files simultaneously since the FortiSandbox has a VM pool. The time to process a file depends on hardware and the number of sandbox VMs used to scan the file. It can take 60 seconds to five minutes to process a file.

FortiSandbox Appliance vs FortiSandbox Cloud

FortiSandbox is available as a physical or virtual appliance (FortiSandbox Appliance), or as a cloud advanced threat protection service integrated with FortiGate (FortiSandbox Cloud).

To select the settings for **Sandbox Inspection**, such as the FortiSandbox type, server, and notifier email, go to **Security Fabric > Settings**.

The table below highlights the supported features of both types of FortiSandbox:

Feature	FortiSandbox Appliance (including VM)	FortiSandbox Cloud
Sandbox inspection for FortiGate	Yes (FortiOS 5.0.4+)	Yes (FortiOS 5.2.3+)
Sandbox inspection for FortiMail	Yes (FortiMail OS 5.1+)	Yes (FortiMail OS 5.3+)
Sandbox inspection for FortiWeb	Yes (FortiWeb OS 5.4+)	Yes (FortiWeb OS 5.5.3+)
Sandbox inspection for FortiClient	Yes (FortiClient 5.4+ for Windows only)	No
Sandbox inspection for network share	Yes	No
Sandbox inspection for ICAP client	Yes	No
Manual File upload for analysis	Yes	Yes
Sniffer mode	Yes	Yes
File Status Feedback and Report	Yes	Yes
Dynamic Threat Database updates for FortiGate	Yes (FortiOS 5.4+)	Yes (FortiOS 5.4+)
Dynamic Threat Database updates for FortiClient	Yes (FortiClient 5.4 for Windows only)	Yes (FortiClient 5.6+ for Windows only)

Note that FortiMail keeps its own Dynamic Threat Database. For more information, see the FortiSandbox documentation.

Sending Files for Sandbox Inspection

Sending files to the FortiSandbox appliance or to FortiSandbox Cloud does not block files immediately. Instead, the files assist in the discovery of new threats and the creation of new signatures to be added to the global FortiGuard AntiVirus database. Files deemed malicious are also immediately added to a custom Malware Package which is downloaded by the FortiGate every two minutes for live detection.

Enable **Sandbox Inspection** by going to **Security Fabric > Settings**. You can also configure the FortiSandbox type, server, and notifier email.

To see options for sending files for sandbox inspection, go to **Security Profiles > AntiVirus**. There are two options for sending files: **None** or **All Supported Files**. If **All Supported Files** is selected, users can withhold files from being submitted for inspection by type or name pattern.

To learn how to connect the FortiSandbox, go to "Using FortiSandbox with a FortiGate" on page 10

Using FortiSandbox with a FortiGate

This section contains information about how to use sandbox inspection with FortiSandbox and FortiGate. It includes the following sections:

- Connecting a FortiGate to FortiSandbox
- FortiSandbox Console

Connecting a FortiGate to FortiSandbox

The procedures for connecting a FortiGate to FortiSandbox differ depending whether you are using FortiSandbox Appliance or FortiSandbox Cloud.

If you are using FortiSandbox in a Security Fabric, consult the Fortinet Cookbook site for the Security Fabric collection of recipes.

Once the FortiGate is connected to FortiSandbox, an AntiVirus profile can be configured to send suspicious files for inspection. Sandbox integration can also be configured, for more information see "Sandbox Integration" on page 12.

Connecting to FortiSandbox Appliance

1. Connect the FortiSandbox Appliance to your FortiGate so that port 1 and port 3 on the FortiSandbox are on different subnets.

FortiSandbox port 3 is used for outgoing communication triggered by the execution of the files under analysis. While the FortiSandbox can accept files through any port, it is recommended to connect port 3 to a dedicated interface on your FortiGate to protect the rest of the network from threats currently being investigated by the FortiSandbox. Note too that port 1 can be used to accept files but is generally reserved for managing the FortiSandbox.

2. FortiSandbox port 3 must be able to connect to the Internet. On the FortiGate, go to **Policy & Objects > IPv4 Policy** and create a policy allowing connections from the FortiSandbox to the Internet (using the isolated interface on the FortiGate mentioned above). On FortiSandbox, network settings for port3 can be configured by going to **Scan Policy > General**.
3. On the FortiSandbox, go to **Network > System Routing** and add static routes for port 1.
4. On the FortiSandbox, go to **Dashboard** and locate the **System Information** widget. Now that the FortiSandbox has Internet access, it can activate its VM licenses. Wait until a green arrow shows up beside **Windows VM** before continuing to the next step.
5. On the FortiGate, go to **Security Fabric > Settings**. Select **Enable Sandbox Inspection** and select **FortiSandbox Appliance.** Set the **IP Address** and enter a **Notifier Email.** If you select **Test Connectivity**, the **Status** shows as **Service is not configured** because the FortiGate has not been authorized to connect to the FortiSandbox.

6. On the FortiSandbox, go to **Scan Input > Device**. **Edit** the entry for the FortiGate. Under **Permissions & Policy > Authorized**, select the checkbox and click **OK** to authorize the FortiGate.
7. On the FortiGate, go to **Security Fabric > Settings** and select **Test Connectivity** for the FortiSandbox. The **Status** now shows that **Service is online**.

Connecting to FortiSandbox Cloud

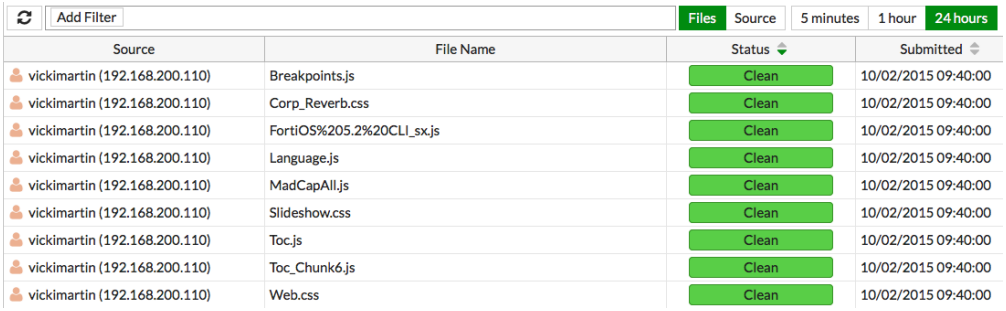
Before you can connect a FortiGate to FortiSandbox Cloud, you need an active FortiCloud account. For more information, see the FortiCloud documentation.

Once you have created a FortiCloud account, sandbox inspection should be enabled by default. To verify this, go to **Security Fabric > Settings**, enable **Sandbox Inspection**, and set to **FortiSandbox Cloud**.

To see the results from FortiSandbox Cloud in the FortiGate logs, go to **Log & Report > Log Settings** and enable **Send Logs to FortiCloud** and set **GUI Preferences** is to display logs from FortiCloud.

FortiSandbox Console

The FortiSandbox console is available at **FortiView > FortiSandbox**. The console displays all samples submitted for inspection. Information on the console can be filtered by checksum, file name, result, source, status, and user name.



If you right-click on an entry, you can choose to **Drill Down to Details**, **Quarantine Source Address**, or **Quarantine FortiClient Device**.

Information about the FortiSandbox database and sandboxing statistics are available at **Security Fabric > Settings** once sandbox inspection is enabled. The **Advanced Threat Protection** dashboard widget shows you the number of files that your FortiGate unit has uploaded or submitted to FortiSandbox.

Refer to FortiSandbox documentation for details on what you can access through the FortiSandbox GUI .

Sandbox Integration

Sandbox integration adds another level to sandbox inspection, allowing you allows you to set up automatic actions to protect your network from files FortiSandbox determines are malicious. These actions include: receiving AntiVirus signature updates from FortiSandbox, adding the originating URL of any malicious file to a blocked URL list, and extending sandbox scanning to FortiClient devices.

This section contains the following topics:

- Overview
- Example Configuration

Overview

FortiSandbox integration involves three different FortiGate security profiles: AntiVirus, Web Filtering, and FortiClient Profiles.

A FortiGate can retrieve scan results and details from FortiSandbox, and also receive antivirus and web filtering signatures to supplement the current signature database. When FortiGate learns from FortiSandbox that an endpoint is infected, the administrator can push instruction for self-quarantine on a registered FortiClient host.

When integrated with a FortiGate unit, the following protocols are supported by FortiSandbox: HTTP, HTTPS, FTP, FTPS, POP3, POP3S, IMAP, IMAPS, SMTPS, MAPI, MAPIS, SMB, and supported IM protocols.

AntiVirus

When FortiSandbox discovers a malicious file, it can create an AntiVirus signature for that file and add that signature to both the local FortiGate malware database and the FortiGuard AntiVirus signature database. Through FortiSandbox integration, this signature can be sent to a FortiGate to block the file from re-entering the network and to prevent the future retransmission of that file to FortiSandbox.

Use of the FortiSandbox AntiVirus database is enabled in an AntiVirus profile, found at **Security Profiles > AntiVirus**. It can also be configured using the following CLI commands:

```
config antivirus profile
   edit <profile>
      set analytics-db enable
   end
```

Web Filtering

FortiSandbox integration can also be used to allow FortiSandbox to add a URL filter blocking the source of a discovered malicious file to the FortiGate's blocked URL list.

Blocking malicious URLs discovered by FortiSandbox is enabled in a Web Filter profile, found at **Security Profiles > Web Filter**. It can also be configured using the following CLI commands:

```
config webfilter profile
   edit <profile>
      config web
```

```
        set blacklist enable
    end
```

FortiClient Profiles

Extended FortiSandbox scanning is currently only supported by FortiClient 5.4 for Windows. It can also only be used with FortiSandbox Appliance.

When extended FortiSandbox scanning is enabled for FortiClient, files downloaded by FortiClient can be sent to the FortiSandbox for inspection. Also, if a suspicious file is discovered, FortiClient can be configured to wait until sandbox inspection is complete before allowing that file to be accessed.

AntiVirus signatures can also be pushed by the FortiGate to FortiClient.

If a FortiClient device attempts to download a file that FortiSandbox discovers is malicious, the FortiSandbox notifies the FortiGate. The administrator can take action to quarantine the device. When a quarantine is in effect, FortiClient cuts off other network traffic from the device directly, preventing it from infecting or scanning the local network. When a device is under quarantine, FortiClient cannot be shutdown or uninstalled. A user is also unable to unregister from the FortiGate that quarantined them, or register to another FortiGate unit. A quarantine can only be lifted by the administrator of the FortiGate where the FortiClient device is registered.

Extending FortiSandbox scanning can by configured in the **Security** settings of a FortiClient Profile, found at **Security Profiles > FortiClient Profiles**. It can also be configured using the following CLI commands:

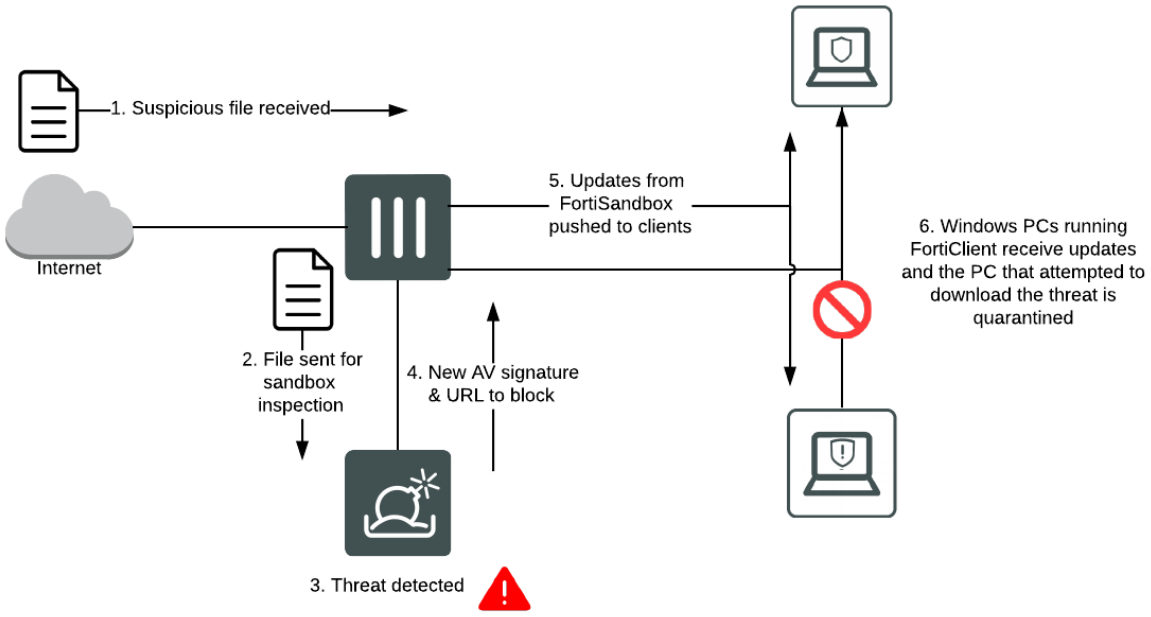
```
config endpoint-control profile
   edit <profile>
      config forticlient-winmac-settings
         set forticlient-av enable
         set av-realtime-protection enable
         set sandbox-analysis enable
         set sandbox-address <address>
      end
```

Extending FortiSandbox scanning can also be configured directly in the FortiClient **AntiVirus** settings. If you are using FortiClient version 5.6+, the **Sandbox Detection** feature can be used to send files to FortiSandbox for analysis without having to install the AntiVirus feature. See the FortiClient 5.6 Administration Guide for details.

The number of files sent from a single device to FortiSandbox can be limited by configuring the submission limit on the FortiSandbox. This allows users to prioritize which devices get the greater share of FortiSandbox resources.

Example Configuration

The following example configuration sets up FortiSandbox integration using AntiVirus, Web Filtering, and a FortiClient profile. This configuration assumes that a connection has already been established between the FortiSandbox Appliance and the FortiGate.



1. Go to **Security Fabric > Settings** and confirm that **Sandbox Inspection** is enabled and the **FortiSandbox Appliance** is connected.
2. Go to **Security Profiles > AntiVirus** and edit the default profile. Under **Inspection Options**, select **All Supported Files** to be sent for inspection and enable **Use FortiSandbox Database**. You have the option of withholding files by name or pattern. Select **Apply**.
3. Go to **Security Profiles > Web Filter** and edit the default profile. Under **Static URL Filter**, enable **Block malicious URLS discovered by FortiSandbox**. Select **Apply**.
4. Go to Security Profiles > FortiClient Profiles and edit the default profile. Under Security Posture Check, enable **Realtime Protection**. Next, enable **Scan with FortiSandbox**. Select **Apply**.
5. Go to **Policy & Objects > IPv4 Policy** and view the policy list. If a policy has AntiVirus and Web Filtering profiles scanning applied, the profiles will be listed in the **Security Profiles** column. If scanning needs to be added to any security policy (excluding the **Implicit Deny** policy) select the **+** button in the **Security Profiles** column for that policy, then select the default **AntiVirus Profile**, the default **Web Filter Profile**, the appropriate **Proxy Options**, and select the **deep-inspection** profile for **SSL/SSH Inspection** (to ensure that encrypted traffic is inspected).
6. Select **OK**.

Results

If your FortiGate discovers a suspicious file, it will be sent to the FortiSandbox. To view information about the files that have been sent on the FortiGate, go to **FortiView > FortiSandbox** to see a list of file names and current status.

To view results on the FortiSandbox, go to the **Dashboard**and view the **Scanning Statistics** widget. There may be a delay before results appear on the FortiSandbox.

Open FortiClient using a Windows PC on the internal network. Make sure it is registered to your FortiGate. Go to the **AntiVirus** tab and open **Settings**. You will see that the **Realtime Protection** settings match the FortiClient profile configured on the FortiGate. These settings cannot be changed using FortiClient.

If a PC running FortiClient downloads a suspicious file that the FortiSandbox determined was malicious, a quarantine would be applied automatically. While the quarantine is in effect, FortiClient cannot be shutdown on the PC. It can not be uninstalled or unregistered from the FortiGate. The quarantine can only be released from the FortiClient Monitor on the FortiGate.

Sandbox Inspection FAQ

The following are some frequently asked questions about using sandbox inspection with FortiSandbox and FortiGate.

Why is the FortiSandbox Cloud option not available when sandbox inspection is enabled?

This option is only available if you have already created a FortiCloud account. For more information, see the FortiCloud documentation.

Why don't results from FortiSandbox Cloud appear in the FortiGate GUI?

Go to **Log & Report > Log Settings** and make sure **Send Logs to FortiCloud** is enabled and **GUI Preferences** is set to **Display Logs from FortiCloud**.

Why are the FortiSandbox Appliance VMs inactive?

Make sure that port 3 on the FortiSandbox has an active Internet connection. This is required in order to active the FortiSandbox VMs.

Why aren't files are being scanned by FortiSandbox?

Make sure an AntiVirus profile that sends files to FortiSandbox is enabled for all policies that require sandbox inspection.

Is FortiSandbox supported by FortiGate when in NAT or Transparent mode?

Yes, both NAT and Transparent mode are supported.

Are FortiGates behind a NAT device supported? If so how many?

Yes, multiple FortiGates can be supported in-line with FortiSandbox. Currently, there is a limitation where the FortiSandbox will see all FortiGates only as one device so there is no way to differentiate reports but all material will be sent.

If the FortiGate has a dynamic IP, will the FortiSandbox automatically update the FortiGate?

Yes. Dynamic IPs™ are supported and the FortiGate will not have to be reconfigured on the FortiSandbox each time.

FORTINET

High Performance Network Security