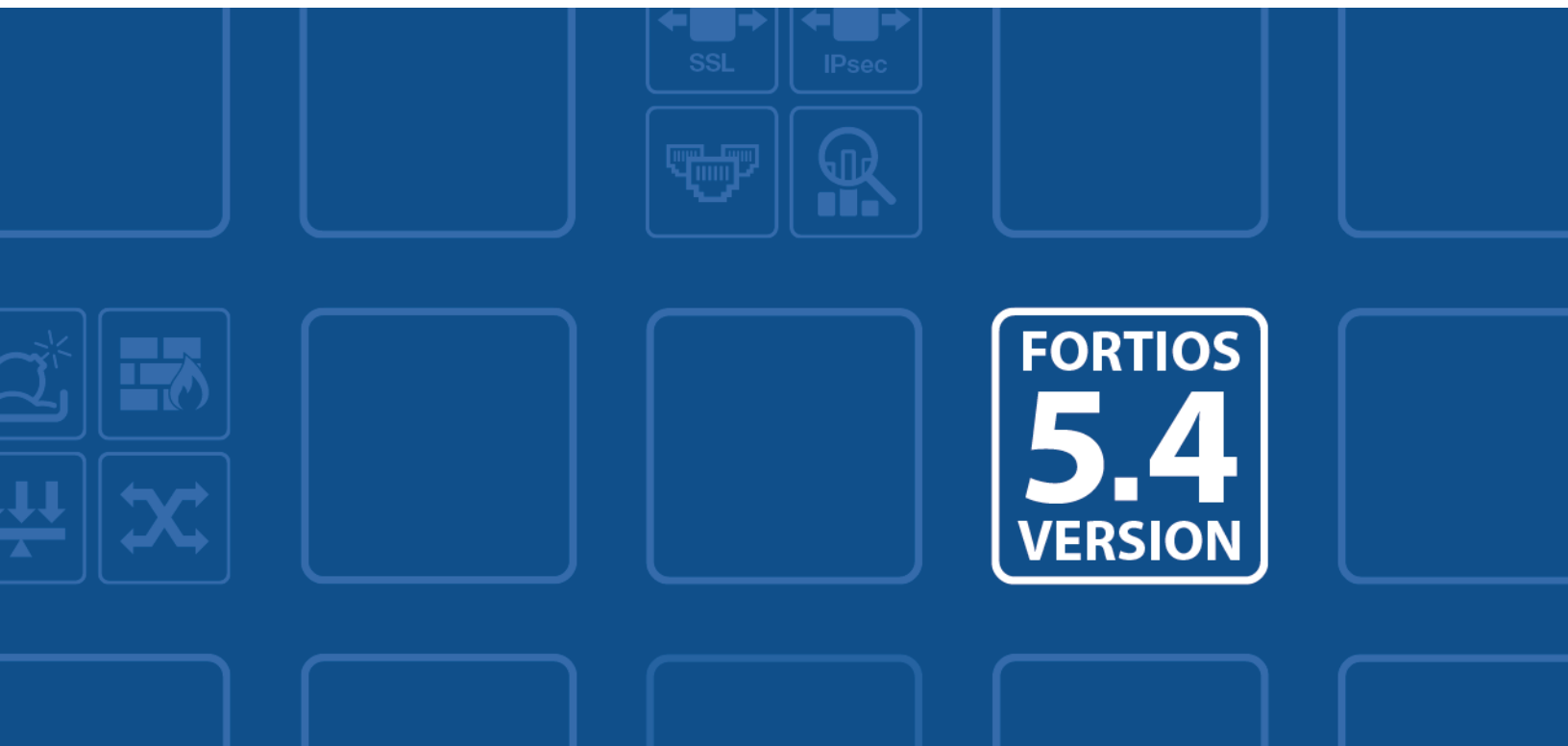
FortiOS™ Handbook - Sandbox Inspection

VERSION 5.4.0



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

END USER LICENSE AGREEMENT

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

FEEDBACK

Email: techdocs@fortinet.com

7/14/2016

FortiOS™ Handbook - Sandbox Inspection

TABLE OF CONTENTS

Change Log

Date	Change Description
July 14, 2016	Clarifications to text regarding malware database and AntiVirus profile configuration
July 11, 2016	Edit to reflect that FortiMail now supported in FortiCloud
June 13, 2016	Updates reflecting changes with FortiOS 5.4.1
March 3, 2016	Initial release

Introduction

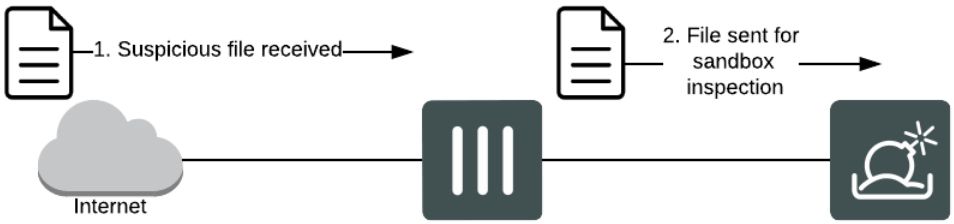
This guide explains how to set up sandbox inspection using FortiSandbox with a FortiGate. It contains the following sections:

- 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.

An Overview of Sandbox Inspection

This section contains information about how Fortinet sandbox inspection works.

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.

When a FortiGate uses sandbox inspection, files are sent to the FortiSandbox. Then the FortiSandbox uses virtual machines (VMs) running different operating systems to test the file, 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.

Sending Files for Sandbox Inspection

Sending files to the FortiSandbox appliance or to FortiCloud 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 sent to the FortiGate every two minutes for live remediation.

Options for sending files for Sandbox Inspection differ between FortiOS 5.4 and FortiOS 5.4.1. Go to **Security Profiles > AntiVirus** to set those options.

FortiOS 5.4

There are three options concerning what type of files can be sent for sandbox inspection: **All Files**, **Suspicious Files**, or **Executable Files**.

All Files is the recommended selection to increase the likelihood of detecting unknown malware.

If **Suspicious Files** is selected, then the FortiGate will examine each file and determine if it should be considered suspicious. A file is deemed suspicious when it does not contain a known threat but has characteristics that suggest it may be malware. The characteristics that determine if a file is suspicious are updated by Fortinet to reflect the current threat climate.

If **Executable Files** is chosen, all executable files will be sent to FortiSandbox while other file types are not inspected.

FortiOS 5.4.1

There are two options for sending files for sandbox inspection: **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.

FortiSandbox Appliance vs FortiCloud

FortiSandbox is available as a physical or virtual appliance (FortiSandbox Appliance), or as a cloud advanced threat protection service integrated with FortiGate (FortiCloud). The table below highlights the supported features of both types of FortiSandbox:

Feature	FortiSandbox Appliance (including VM)	FortiCloud
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+)	No
Sandbox inspection for FortiClient	Yes (FortiClient 5.4 for Windows only)	No
Manual File upload for analysis	Yes	No
Sniffer mode	Yes	No
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 FortiMail	Yes (FortiMail OS 5.3+)	Yes (FortiMail OS 5.3+)
Dynamic Threat Database updates for FortiClient	Yes (FortiClient 5.4 for Windows only)	No

For more information, see the FortiSandbox documentation.

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
- The FortiSandbox Dashboard

Connecting a FortiGate to FortiSandbox

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

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. It is recommended to connect this port to a dedicated interface on your FortiGate to protect the rest of the network from threats currently being investigated by 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).
3. On the FortiSandbox, go to **System > Network > Static Routing** and add static routes for port 1 and port 3.
4. On the FortiSandbox, go to **System > Status** 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 **System > Cooperative Security Fabric**. 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 **File-based Detection > File Input > Device**. Edit the entry for the FortiGate. Under **Permissions,** enable **Authorized**.
7. On the FortiGate, go to **System > Cooperative Security Fabric** and for FortiSandbox select **Test Connectivity**. The **Status** now shows that **Service is online**.

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 10.

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.

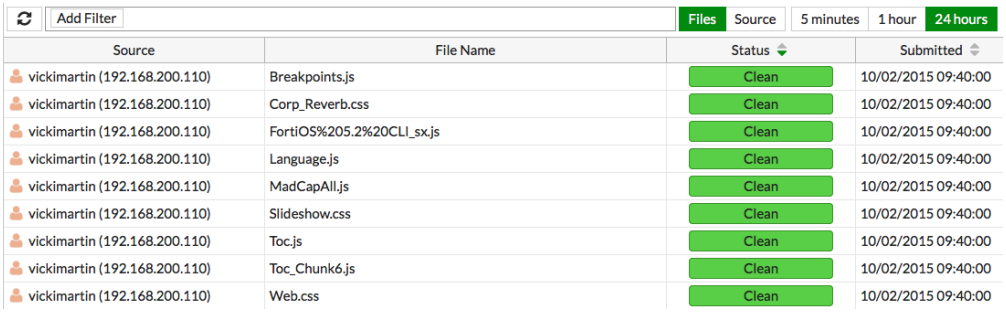
Once you have created a FortiCloud account, sandbox inspection should be enabled by default. To verify this, go to **System > Cooperative Security Fabric**and make sure **Enable Sandbox Inspection** is selected and set to **FortiSandbox Cloud**.

To see the results from FortiSandbox Cloud in the FortiGate logs, 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**.

Now that 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 10.

The FortiSandbox Dashboard

The FortiSandbox dashboard is available from **FortiView > FortiSandbox**. The dashboard shows all samples submitted for inspection. Information on the dashboard 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 also available at **System > Cooperative Security Fabric** 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.

Information can also be found by accessing FortiSandbox. For more information, please refer to the FortiSandbox documentation.

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:

See the What's New chapter on FortiSandbox Integration for changes made in FortiOS releases 5.4.1 and later.

Overview

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

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.

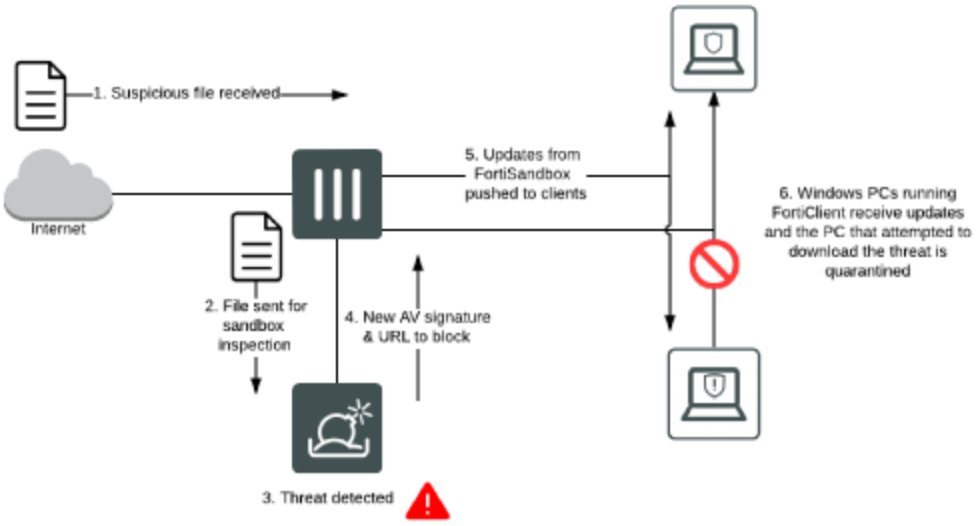
If a FortiClient device attempts to download a file that FortiSandbox discovers is malicious, the FortiSandbox notifies the FortiGate. The administrator can take action to quarantine the device. When a quarantine is in effect, FortiClient cuts off other network traffic from the device directly, preventing 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 scan-download-file enable
         set sandbox-scan enable
         set sandbox-address <address>
         set wait-sandbox-result {enable | disable}
         set use-sandbox-signature {enable | disable}
      end
```

Extending FortiSandbox scanning can also be configured directly in the FortiClient **AntiVirus** settings.

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 Profiles > AntiVirus** and edit the default profile. Under **Inspection Options**, enable both **Send Files to FortiSandbox Appliance for Inspection** and **Use FortiSandbox Database**. Select **Apply**.
2. Go to **Security Profiles > Web Filter** and edit the default profile. Under **Static URL Filter**, enable **Block malicious URLS discovered by FortiSandbox**. Select **Apply**.
3. Go to **Security Profiles > FortiClient Profiles** and edit the default profile. Under **AntiVirus**, enable **Realtime Protection**, then enable **Scan Downloads**, followed by **Scan with FortiSandbox**. Enter the IP of the FortiSandbox, then enable **Use FortiSandbox signatures**. Select **Apply**.
4. Go to **Policy & Objects > IPv4 Policy** and view the policy list. If a policy has AntiVirus and Web Filtering 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 the **deep-inspection** profile for **SSL Inspection Options** (to ensure that encrypted traffic is inspected).
5. Select **OK**.

Results

If your FortiGate discovers a suspicious file, it will now 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 **System > Status** 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 **AntiVirus > Realtime Protection Enabled** and edit the 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.