FortiSandbox

Sizing Guide

FortiSandbox is a multi featured File/URI processing platform intended to reveal malware hidden inside of ordinary or innocuous looking files. FortiSandbox will accept files from multiple feeds simultaneously. The size of your FortiSandbox is determined by the total number of files it is expected to process per hour.

There are many deployment options and input mechanisms/feeds available to FortiSandbox:

- Integrated with devices such as FortiGate and FortiMail*
- Network mirror/span/tap sniffing of File/URI/CC*
- Network file share (CIFS/NFS) scanning on-demand/scheduled
- Direct on-demand File/URI submission via GUI and/or API

*The primary methods of the FSA receiving files are via “Integrated device” and “Wire sniffing”.

Sizing Definitions

Integrated:

- What is the total number of integrated FGT/FML devices?
- How many policies will be FSA activated on each device?

You can get an idea of how many files the FortiGate is processing by monitoring the ATP widget. You can then do your size planning by making some educated guesses. For example, if your firewall processes 1000 files per hour, and has 100 policies, you may be able to enable sandboxing integration for 1 – 5 policies on the 1000D and 5 -10 rules on the 3000D (depending on the volume each policy processes).

Wire sniffing (stand alone):

- How many span/mirror/tap ports do you want to monitor?
- What protocols do you plan to monitor (FTP/HTTP/IMAP/POP3/SMB/SMTP)?

If you plan to deploy the FSA stand alone, the 1000D will process up to 1.2Gbs, and the 3000D will process up to 3.8Gbs of sustained traffic. The max number of AV and VM processed file recommendations in the datasheet still apply.

Network file share scan:

- How many file share locations?
- What is the average size of each file share location?
- What types of files do you want to scan?

If you plan to scan CIFS/NFS file shares, consider breaking the scan down into small targeted segments and file types, and stagger the scheduling overnight.

While the official FortiSandbox datasheet lists the details of the overall functionality, this document is intended to assist in sizing your FortiSandbox to your environment.

Summary

Please determine the mechanisms you will be using to send files to the FortiSandbox to determine the sizing. When implementing FortiSandbox, it is highly recommended to incrementally add feeds to ensure you are not overwhelming the device.

	FSA-1000D	FSA-3000D	FortiSandbox-VM
Integrated device policies			
One to Ten	✓	✓	✓
Ten to Fifty		✓	✓
Fifty to One Hundred			✓
Network sniffer volume			
1Gb	✓	✓	✓
10Gb		✓	✓
Users			
Up to 100	✓	✓	✓
Up to 500		✓	✓
500+			✓

Files received from integrated devices such as FortiGate (FGT) and FortiMail (FML) will already have had an AntiVirus (AV) scan done on them. These files are ALL likely to be executed/opened in a Virtual Machine (VM) - unless there is a matching FSA "Cloud" signature or the file is a duplicate.

Files sniffed from the wire will be scanned by the AV engine and may also need to be executed/opened in a VM. The AV engine is designed to scan objects with a very high degree of accuracy and performance. For the files that are not detected by the AV engine, the FSA virtual engine will then process the file through a VM. This is one of the reasons why you see the different capacity numbers for the "AV Scanning" and "VM Sandboxing" of files on the last page of the data sheet.

If you are integrating a FSA with a FGT, you can get an idea of how many files the FGT is processing per hour/day by tracking the "Number of files scanned" value in the "Advanced Threat Protection Statistics" widget.

If you are integrating a FSA with FML you can get an idea of how many attachments the FML is processing by setting up a simple content filter to track the number of attachments in/outbound.

If you plan to use the FSA sniffer, the same total hourly number of AV and VM processed file guidelines apply.

What does this mean, in real world terms? A simple example is if a FGT is processing up to around 160/560 files per hour, you would recommend pairing it with a FSA 1000D/3000D. Your individual sizing exercises are however likely to be more complex.

You have some control over the total number of files being sent to the FSA from an integrated FGT/FML by enabling the sandboxing integration per individual policy. For example, if your firewall processes 1000 files per hour and has 100 policies, you may be able to enable sandboxing in an AV profile on 1 – 2 policies for the FSA 1000D, and 5 – 6 policies for the FSA 3000D.

FGT v5.2.x has an option in any AV profile to either enable "send all files" or "send suspicious files" to the FSA. It is highly recommended to ALWAYS use the "send all files" option in your FGT AV profiles. The "send suspicious file" option is being removed from the AV profile configuration in future FGT firmware releases. The reason is that sending only suspicious files greatly inhibits the ability to find unknown malware – which most of the time does not look suspicious.

GLOBAL HEADQUARTERS
Fortinet Inc.
899 Kifer Road
Sunnyvale, CA 94086
United States
Tel: +1.408.235.7700
www.fortinet.com/sales

EMEA SALES OFFICE
120 rue Albert Caquot
06560, Sophia Antipolis,
France
Tel: +33.4.8987.0510

APAC SALES OFFICE
300 Beach Road 20-01
The Concourse
Singapore 199555
Tel: +65.6513.3730

LATIN AMERICA SALES OFFICE
Paseo de la Reforma 412 piso 16
Col. Juarez
C.P. 06600
México D.F.
Tel: 011-52-(55) 5524-8428

Copyright © 2015 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 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. 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.

June 12, 2015