



FortiOS - Docker Cookbook

Version 6.4

FORTINET DOCUMENT LIBRARY

<https://docs.fortinet.com>

FORTINET VIDEO GUIDE

<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/support-and-training/training.html>

NSE INSTITUTE

<https://training.fortinet.com>

FORTIGUARD CENTER

<https://fortiguard.com/>

END USER LICENSE AGREEMENT

<https://www.fortinet.com/doc/legal/EULA.pdf>

FEEDBACK

Email: techdoc@fortinet.com



March 31, 2020

FortiOS 6.4 Docker Cookbook

01-640-619455-20200331

TABLE OF CONTENTS

FortiGate-VM on a Docker environment	4
Change log	5

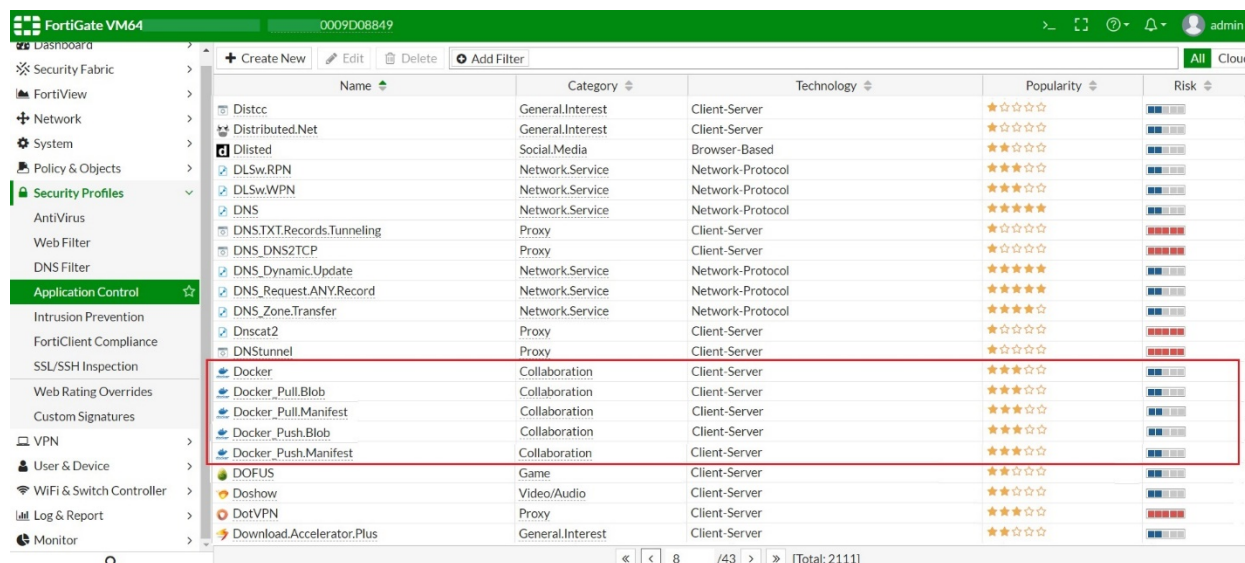
FortiGate-VM on a Docker environment

Unlike FortiWeb-VM, you cannot deploy FortiGate-VM as a Docker container. However, FortiGate-VM can protect various resources in the Docker environment.

Docker's popularity has seen an increasing volume of activities of downloading and uploading Docker images and their manifests over the Internet. Since the majority of the Docker images in the public registries are vulnerable, it is important to ensure that you only download images from a source where they have already been scanned for vulnerabilities. To help enforce this policy, FortiGate application control has added signatures for Docker traffic.

Application control signature	Indication of an attempt to:
Docker	Access Docker.
Docker_Pull.Blob	Pull a blob from Docker.
Docker_Push.Blob	Push a blob onto Docker.
Docker_Pull.Manifest	Pull a manifest from Docker.
Docker_Push.Manifest	Push a manifest onto Docker.

By updating the signature after initial FortiGate deployment, you should see the Docker-related application controls added in *Security Profiles > Application Control*.



You can configure firewall policies to allow pulls and pushes with known clean private Docker registries using their IP addresses (or IP addresses except for malicious and blacklisted ones) as either sources or destinations while having awareness of Docker-related application in traffic.

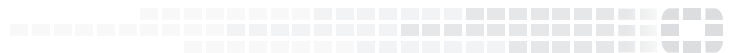
Apart from application control, the FortiGate also scans all traffic in the Docker environment for vulnerabilities and file-based threats using Intrusion Prevention Service and Advanced Malware Protection.

Change log

Date	Change Description
2020-03-31	Initial release.



FORTINET®



Copyright© 2020 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, 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. In no event does Fortinet make any commitment related to future deliverables, features or development, and circumstances may change such that any forward-looking statements herein are not accurate. 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.