FURTINET

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

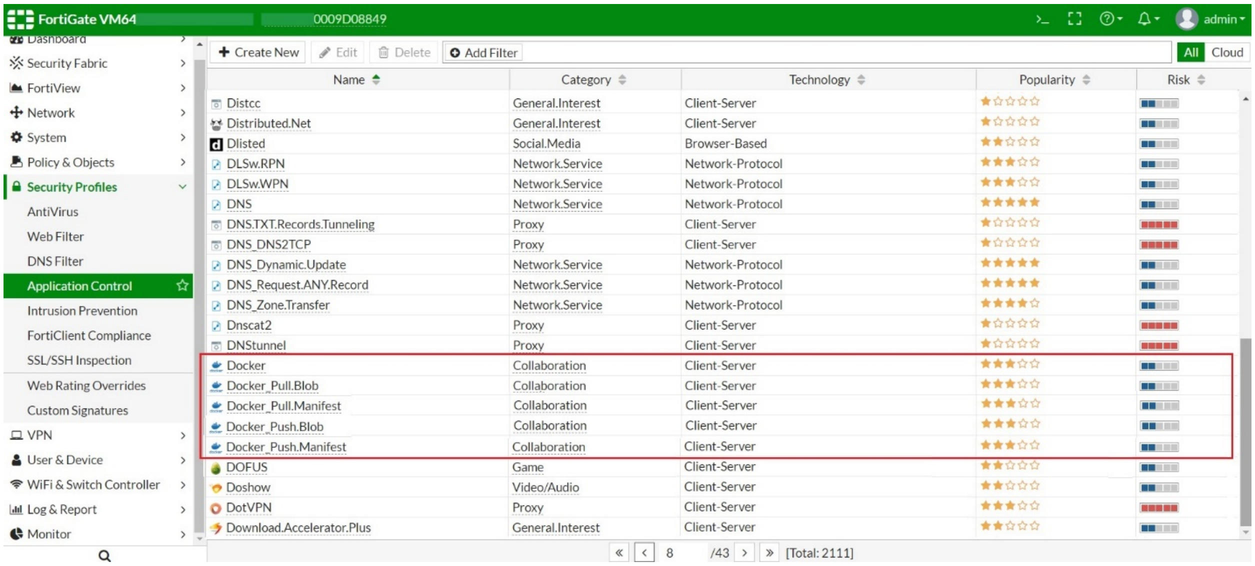
FortiGate-VM on a Docker environment

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*.



Name	Category	Technology	Popularity	Risk
Distcc	General.Interest	Client-Server	★☆☆☆☆	■■□□□
Distributed.Net	General.Interest	Client-Server	★☆☆☆☆	■■□□□
Dlisted	Social.Media	Browser-Based	★★☆☆☆	■■□□□
DLSw.RPN	Network.Service	Network-Protocol	★★★☆☆	■■□□□
DLSw.WPN	Network.Service	Network-Protocol	★★★☆☆	■■□□□
DNS	Network.Service	Network-Protocol	★★★★★	■■□□□
DNS.TXT.Records.Tunneling	Proxy	Client-Server	★☆☆☆☆	■■■■■
DNS_DNS2TCP	Proxy	Client-Server	★☆☆☆☆	■■■■■
DNS_Dynamic.Update	Network.Service	Network-Protocol	★★★★★	■■□□□
DNS_Request.ANY.Record	Network.Service	Network-Protocol	★★★★★	■■□□□
DNS_Zone.Transfer	Network.Service	Network-Protocol	★★★★☆	■■□□□
Dnscat2	Proxy	Client-Server	★☆☆☆☆	■■■■■
DNStunnel	Proxy	Client-Server	★☆☆☆☆	■■■■■
Docker	Collaboration	Client-Server	★★★☆☆	■■□□□
Docker_Pull.Blob	Collaboration	Client-Server	★★★☆☆	■■□□□
Docker_Pull.Manifest	Collaboration	Client-Server	★★★☆☆	■■□□□
Docker_Push.Blob	Collaboration	Client-Server	★★★☆☆	■■□□□
Docker_Push.Manifest	Collaboration	Client-Server	★★★☆☆	■■□□□
DOFUS	Game	Client-Server	★★☆☆☆	■■□□□
Doshow	Video/Audio	Client-Server	★★☆☆☆	■■□□□
DotVPN	Proxy	Client-Server	★★★☆☆	■■■■■
Download.Accelerator.Plus	General.Interest	Client-Server	★★☆☆☆	■■□□□

« < 8 /43 > » [Total: 2111]

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.