FortiADC Release Notes

Version 5.2.5

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

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

Monday, September 9, 2019

FortiADC 5.2.5 Release Notes

First Edition

TABLE OF CONTENTS

Change Log

Date	Change Description
09/09/2019	FortiADC 5.2.5 Release Notes initial release.

Introduction

This *Release Notes* covers the new features, enhancements, known issues, and resolved issues of FortiADC™ Version 5.2.5, Build 0460.

To upgrade to FortiADC 5.2.5, see FortiADC Upgrade Instructions.

FortiADC provides load balancing, both locally and globally, and application delivery control. For more information, visit: http://docs.fortinet.com/fortiadc-d-series/.

What's new

FortiADC 5.2.5 is a patch release only; no new feature or enhancement has been implemented in this release.

Upgrade notes

Backup config file

After upgrading to V5.2.5, please discard the old backup files at 5.2.x before, then do the backup in V5.2.5 again; it should work now.

CVE-2017-17544

To fix the vulnerability CVE-2017-17544, only super admin are allowed to restore configuration from 5.2.5.

Hyper-V

New template for Hyper-V 2016/2019 support.

Statistics data format converting

After upgrading to V5.2.5, the old statistics data will not be converted to the new version automatically; instead, there is a warning on the top right position. The client may click the warning to start the converting. However, the converting may consume CPU and memory resources. Only clients upgrading from prior to 5.2.0 can have old statistic data.

allow-ssl-version

There is an old SSL version in the allow-ssl-version config that is not recommend; but the client may have configured it before. This is removed when you upgrade from 5.0.x to 5.1.x/5.2.x. The client may need to add it back manually for compatibility.

Adjust boot partition

VM's prior to 5.1.x had a size limit to the boot partition. Thus, you need to upgrade to 5.1.x, first, to adjust the boot partition. Then you can upgrade to 5.2.5. Otherwise it will report "Unmatched partition size."

No such issue for physical platforms.

Dynamic auth feature

It is suggested that the customer should only enable "dynamic auth feature" on RADIUS accounting virtual servers.

Hardware and VM support

FortiADC 5.2.5 supports the following hardware models:

- FortiADC 200D
- FortiADC 300D
- FortiADC 400D
- FortiADC 700D
- FortiADC 1500D
- FortiADC 2000D
- FortiADC 4000D
- FortiADC 60F (without HSM, PageSpeed, and AV features)
- FortiADC 100F
- FortiADC 200F
- FortiADC 1000F
- FortiADC 2000F
- FortiADC 4000F

FortiADC Release 5.2.5 supports deployment of FortiADC-VM in the following virtual machine environments:

VM environment	Tested Versions
VMware	ESXi 3.5, 4.x, 5.0, 5.1, 5.5, 6.0, 6.5, 6.7
Microsoft Hyper-V	Windows Server 2012 R2
KVM	Linux version 3.19.0 qemu-img v2.0.0, qemu-img v2.2
Citrix Xen	XenServer 6.5.0
Xen Project Hypervisor	4.4.2, 4.5

Resolved issues

This section lists the major known issues that have been resolved in this 5.2.5 release. For inquiries about particular bugs, please contact Fortinet Customer Service & Support.

Table 1: Resolved issues

Bug ID	Description
0563188	Removed the extra warning log "no source pool configured" for a L4 VS which has already configured NAT source pool
0576022	Improved of backend shared-memory for GUI
0577439	HA peer left and join and Arp conflicts seen in event log
0557149	The expiration of the persistence on the peer side displays incorrectly
0572451	Added CLI option to supress HTTP code 400 error in HTTP response
0568196	CVE-2019-11478 Excess Resource Usage (all Linux versions) and SACK Slowness (Linux < 4.15)
0568192	SACK Panic attack: CVE-2019-11477
0568014	Improvement: Should match country if the source DNS traffic is from different region especially using G20 GEO-IP library
0574789	A configuration which has a key-file with no pass phrase cannot be restored properly using the backup file.
0565447	Improvement: Support AWS Type M4, M5, C5
0568535	Changed GLB cname target name limit from 48 to 255
0557573	FortiADC OCI SDN connector needs to cover all OCI regions
0517382	Secure flag support in SSL/TLS HTTPS Cookies to avoid Cookie leaking
0571886	There could be extremely strange traffic triggering the L4-VS crash
0571274	Change the default MTU back to 1500 on KVM platform.
0572647	New CLI command to update and check IRDB version
0568810	[FUSE] Confused log info "DROPPED DUE TO CONN_SCHED_UNREACH"

Bug ID	Description
0525665	FortiADC uses DH public key size 127 bytes in DHE_RSA Client Key Exchange message during Healthcheck, causing failures.
0570321	ADC on AWS(China) has 6% ICMP packet loss, and once "dia sniffer packet" is started up, packet loss disappears.
0554087	CVE-2018-5743: Limiting simultaneous TCP clients is ineffective
0540942	[Security release Bind] Versions 9.11.5-P4 and 9.12.3-P4 of Bind are avalaible
0563296	LDAP Fetch is not working after upgrading to 5.x
0569024	Xen-open platform default logdisk should be changed to 30G
0562684	FortiADC Security Fabric API token is not persistent
0568261	Added support for KVM image deploying on ApacheCloudStack
0566984	Added Comment/ Notes filed for Admin IDs
0564257	Fortiview session filter resets after refresh

Known issues

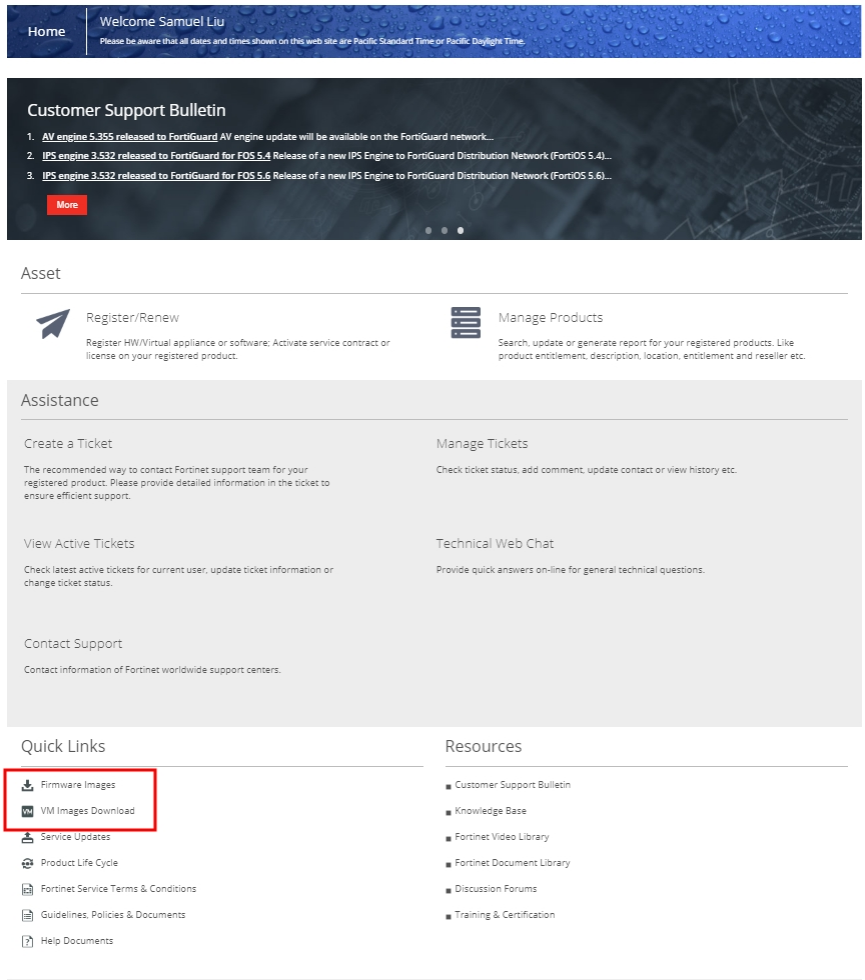
There are no known issues discovered in FortiADC 5.2.5 release. For inquiries about particular bugs, please contact Fortinet Customer Service & Support.

Image checksums

To verify the integrity of the firmware file, use a checksum tool and compute the firmware file's MD5 checksum. Compare it with the checksum indicated by Fortinet. If the checksums match, the file is intact.

MD5 checksums for Fortinet software and firmware releases are available from Fortinet Customer Service & Support. After logging in to the web site, near the bottom of the page, click the Firmware Image Checksums button. (The button appears only if one or more of your devices has a current support contract.) In the File Name field, enter the firmware image file name including its extension, then click Get Checksum Code.

Figure 1: Customer Service & Support image checksum tool



Copyright© 2019 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.