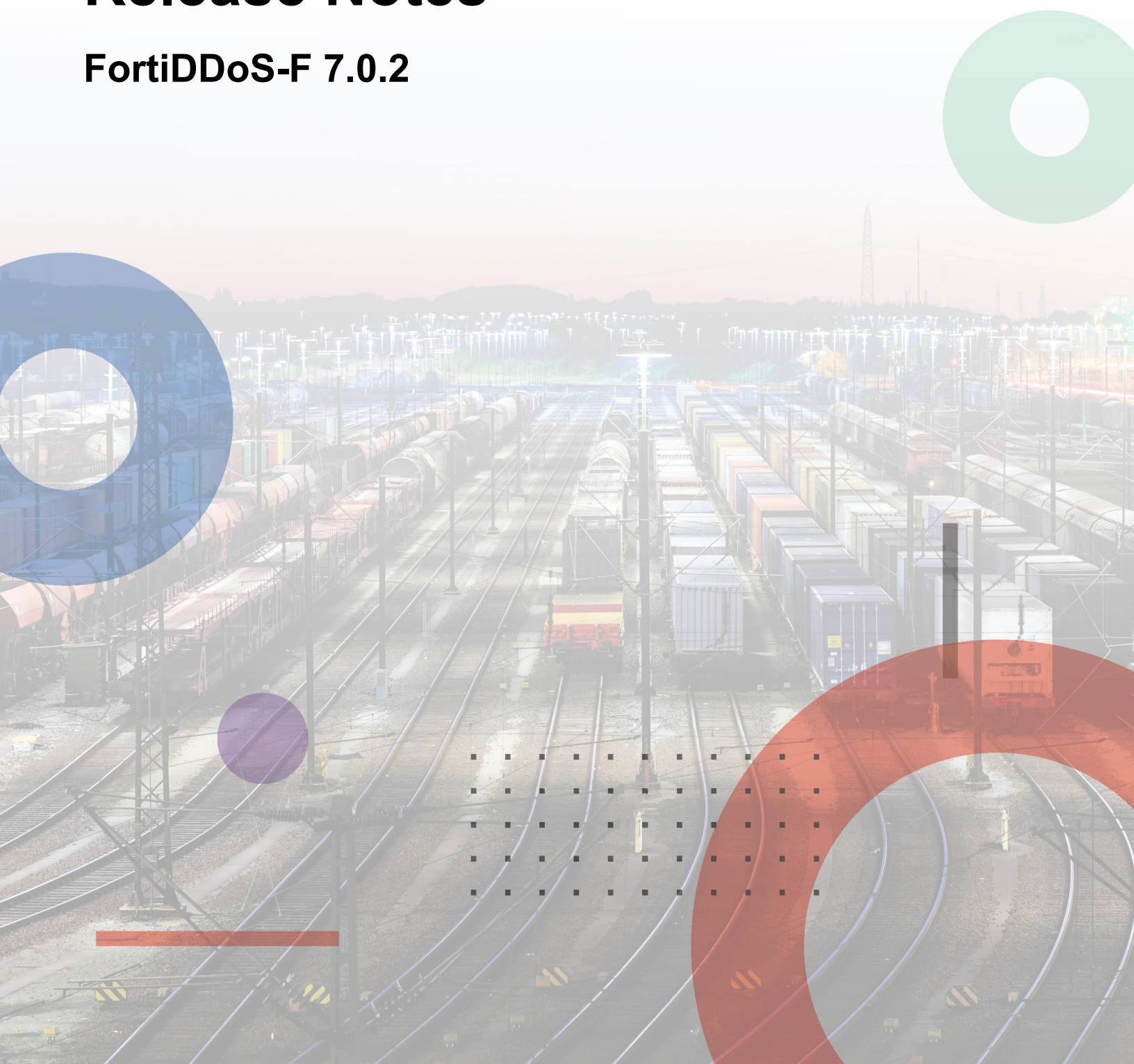
Release Notes

FortiDDoS-F 7.0.2



FORTINET DOCUMENT LIBRARY
https://docs.fortinet.com

FORTINET VIDEO LIBRARY
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/training-certification

FORTINET TRAINING INSTITUTE
https://training.fortinet.com

FORTIGUARD LABS
https://www.fortiguard.com

END USER LICENSE AGREEMENT
https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK
Email: techdoc@fortinet.com

August 2, 2024
FortiDDoS-F 7.0.2 Release Notes

TABLE OF CONTENTS

Change Log

Date	Change Description
August 2, 2024	FortiDDoS-F 7.0.2 Release Notes initial release

Introduction

This Release Notes covers the new features, enhancements, resolved issues and known issues of FortiDDoS version 7.0.2 build 0722.

Special Notes

GUI changes on upgrade from releases below 7.0.1

- GUI access via TLS 1.1 will be disabled after upgrade to 7.0.1 as a security improvement. The option can be re-enabled by the user if desired.

  After upgrade, always open the GUI via a private browser window or refresh the browser cache.
- On upgrade to 7.0.1, the existing LQ table is replaced by a new, much larger, and more granular table for improved mitigation.

  Existing entries are deleted.

  DNS Allowlists or Blocklists are not affected.

  Fortinet strongly recommends placing any SPP using LQ in Detection Mode for upgrade and allowing LQ to learn for at least one day on Authoritative DNS Servers before returning to Prevention Mode. For details, contact Fortinet.
- The Report period of *Last 30 Days* has been removed as redundant with *Last Month*. Before upgrading, check *Log & Report* > *Log Configurations* for Reports with Last 30 Days selected and change them to Last Month.

Manual traffic bypass will not enable in Fail Closed Mode

Global Protection > *Deployment* > *Power Off Bypass Mode* operates correctly in Fail Closed Mode for all F-Series models. However, manual traffic bypass cannot be enabled when the Power Off Bypass Mode is in Fail Closed Mode.

Workaround:
Temporarily place the system into Fail Open Mode, then manually bypass the traffic using either the GUI (Dashboard > System Information panel > Bypass Status link) or CLI (`execute bypass-traffic enable`). After returning FortiDDoS to inline, change the Power Off Bypass Mode back to Fail Closed Mode.

Monitor > *TRAFFIC MONITOR* > *Subnets* graphs affected by upgrade

The following **only** affects the *Monitor* > *TRAFFIC MONITOR* > *Subnets* graphs. All other graphs retain all previous information:

If you are upgrading from a Release lower than 6.5.0, the Round Robin Databases used for these graphs (all protected subnets for all SPPs) are modified during the upgrade and all previous data is deleted. New data will display in the next 5-minute reporting period after upgrade. This does not affect on any other Monitor graph.

See above Special Note. If the system is in Fail Closed Mode, change the setting to Fail Open Mode. Afterwards, place FortiDDoS into Bypass mode. You can do this via GUI from *Dashboard* > *Status* > *System Information* > *Bypass Status* Inline/Bypass link or using CLI:

```
FortiddoS #execute bypass-traffic enable
This operation will enable traffic bypass!
Do you want to continue? (y/n) y
```

It is recommended to perform upgrades in a maintenance window to avoid disrupting other network settings such as OSPF, RSTP and BGP that affect traffic when the physical ports are changed from inline to bypass and back to inline.

After the upgrade is complete, FortiDDoS will return to inline mode. As above, if system is normally in Fail Closed Mode, change that setting back to Fail Closed.

Ensure to clear your browser cache (or operate in incognito mode) after a firmware upgrade. The GUI is coded in Javascript in the browser and code changes in the system do not automatically signal the browser to rebuild the GUI. Changes to the GUI will not appear until the cache is cleared. If the cache is not cleared, you may see misaligned tables or entire Dashboard panels missing or appearing in the wrong place.

What's new

There are no new features in FortiDDoS-F 7.0.2.

Hardware and VM support

FortiDDoS 7.0.2 supports the following hardware models:

- FortiDDoS 200F
- FortiDDoS 1500F
- FortiDdoS 1500F-LR
- FortiDDoS 2000F
- FortiDDoS 3000F

FortiDDoS 7.0.2 is NOT compatible with any FortiDDoS A- / B- / E-Series hardware.

FortiDDoS Release 7.0.2 supports deployment of FortiDDoS-VM in the following virtual machine environments:

- VMware
- KVM

Note: FortiDDoS VMs are not suitable for deployments in public cloud environments such as AWS, Azure or Google Cloud. The firmware will “work” but since FortiDDoS has no IP addresses on its data ports, there is no way to direct traffic to or through it. FortiDDoS must be installed on physical links.

Resolved issues

There are no resolved issues in this release.

Common Vulnerabilities and Exposures

For more information, visit https://www.fortiguard.com/psirt.

Bug ID	Description
1051908	FortiDDoS-F 7.0.2 is no longer vulnerable to CVE-2024-6387

Known issues

This section lists the known issues in FortiDDoS-F 7.0.2 release. For inquiries about particular bugs, please contact Fortinet Customer Service & Support.

Bug ID	Description
0915076	Security Fabric integration with FortiOS is not operational due to changes in the FortiOS API. This will return in a future release.
0693789	When FortiDDoS-VM is operating on a virtual machine with underlying hardware supporting SR-IOV, disabling ports leads to unexpected results.
0678445	Purging a large number of ACLs from an SPP can take more than 30 seconds with no progress indication.
0882029	From Release 6.5.0, graphs do not correctly display Y-axis units when that axis is set to Logarithmic. Instead of pps or bps rates, only 1,2,3, etc are shown on the Y-axis. Tool tip information is correct. Fortinet is working with the graph code provider to correct this in a later release.
0904954	After saving SPP or Global ACL Lists, re-ordering will only work for 1 step up or down from current location in the list.
0918768 0923612 0924121	Within 20 seconds of the end of any 5-minute reporting/graphing period, drops may not be graphed correctly but shown in the next reporting period where no traffic may be present.
942816	FortiDDoS VM manual force FortiGuard update will not work. There is a workaround via shell which will be documented.
928875	Virtual Machines (VM) cannot control bypass modes for the server NICs (even if they have bypass NICs). VMs will always fail closed. Use an external Bypass Bridge for Fail-Open.
1002526	FortiDDoS 2000F 40G QSFP+ TRasceievers are not working correctly. This problem is fixed but requires an RMA for any systems shipped prior to 2024-05. Please contact FortiCare for confirmation.
1011488	DNS Known Opcode Anomalies are shown as DNS Header Anomaly drops. This is design Intent and won't be changed. It is documented in the 7.0.1 Handbook.
1016628	VMs, to save CPU, report all traffic on UDP Ports from 10240-65535 on Port 10240. Adding UDP Service Ports above 10240 does not create additional ranges, nor change any reporting. This is design intent and documented.
995550	If DNS Cache in DNS Profiles are enabled for different SPPs, drops associated with any SPP will be shown for one SPP only. DNS Cache is normally not enabled and should only be used with expert advice.
961369	Manipulating table column configurations can occasionally produce unexpected data table error messages. Refreshing the browser recovers the table.

Bug ID	Description
N/A	FortiDDoS F-Series Cloud Signaling is not optimized with our current Cloud DDoS partner. Contact Fortinet for support.
1059821	Long FQDNs in DNS LQ Populate result in dataplane resets. If using DNS LQ Populate, please set the Max FQDN Length to 64.

Upgrade notes

VM Platforms

On the VM platform, to avoid the VMware network broadcast storm for the new deployment, each WAN/LAN interface pair is disabled by default so that traffic will not pass through.

In the initial deployment, please remember to enable the WAN/LAN interface pair via CLI.

```
# config system l2-interface-pair
# edit l2-port1-port2
# set status enable
# next
# end
```

Hardware Platforms

On upgrade, whether the system is set to Fail-Open or manually forced into the bypass state, traffic will be blocked for a few seconds on the transition from bypass to inline when the upgrade is complete.

Upgrades should be done in a maintenance window or traffic should be diverted.

After upgrade

Check the integrity of the system Service Protection Policies (SPPs) using the following CLI commands.

`diagnose debug rrd_files_check`

Output:

`Global expected:5, found:5` (this is the global SPP)

`SPP:0 expected:1857, found:1857` (this SPP is used internally)

`SPP:1 expected:1857, found:1857` (this is the default SPP)

`SPP:2 expected:1857, found:1857`

`SPP:3 expected:1857, found:1857`

`SPP:4 expected:1857, found:1857` (Maximum SPPs for VM-04)

`SPP:5 expected:1857, found:1857`

`SPP:6 expected:1857, found:1857`

`SPP:7 expected:1857, found:1857`

`SPP:8 expected:1857, found:1857` (Maximum SPPs for 200F/VM-08)

`SPP:9 expected:1857, found:1857`

```
SPP:10 expected:1857, found:1857
SPP:11 expected:1857, found:1857
SPP:12 expected:1857, found:1857
SPP:13 expected:1857, found:1857
SPP:14 expected:1857, found:1857
SPP:15 expected:1857, found:1857
SPP:16 expected:1857, found:1857
```
(Maximum SPPs for 200F/1500F/1500F-LR/3000F/VM-16)

If the expected and found numbers above do not match (they may not be 1857 as above, but must match), you must follow the directions below to recreate/reset the RRDs.

Recreating/resetting the SPP RRDs removes all previous traffic and drops graphing information for that SPP. However, Logs are retained. If you are unsure on how to proceed, contact FortiCare for support.

Repair the SPP using the following CLI commands.

If SPP-0 is missing or SPP-0 RRD is missing:

```
execute backup-rrd-reset
```

It is important to repair this SPP-0 RRD first if the expected/found numbers do not match. This SPP is used to re-build SPPs 1-4/8/16.

If one or a few SPPs from 1-4/8/16 are missing RRDs:

`execute spp-rrd-reset spp <rule_name>` (where rule_name is the textual name from the GUI)

If many SPPs are missing RRDs:

```
execute rrd-reset all
```

If Global is missing RRDs:

```
execute global-rrd-reset
```

www.fortinet.com