Release Notes

FortiDDoS-F 7.0.3

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

September 27, 2024
FortiDDoS-F 7.0.3 Release Notes

TABLE OF CONTENTS

Change Log

Date	Change Description
September 27, 2024	FortiDDoS-F 7.0.3 Release Notes initial release

Introduction

This Release Notes covers the new features, enhancements, resolved issues and known issues of FortiDDoS version 7.0.3 build 0740.

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

FortiDDoS-F7.0.3 offers the following new features and enhancements:

GUI and Graph updates

The following updates were made to the FortiDDoS-F GUI and graphs:

General

- Sort arrows now function correctly across all tables.
- Added time-line graphs for *Data Path Resources*, allowing viewable periods from 1-hour to 1-year.
- The *Dashboard> Status > System Resources* chart is rotated to vertical bars for consistent presentation in Chrome, Edge, Firefox, and Safari browsers.

Logs and Reports:

- The right-most data point on all graphs shows the last reported traffic/drop time for improved clarity.
- The Reports configuration list page now allows you to clone any report to simplify configuration.
- Additional SYN-ACK graphs to improve troubleshooting and traffic analysis.
- Search bar is removed from *Attacked Destinations Report* page since all reports show on one page.
- GUI access to *Log & Report > LOG ACCESS > Log Backup* for backing up the MySQL database has been removed due to low demand. However, the MySQL database can still be backed up using the CLI.
- *Estimated Threshold graph* has been added for *SYN/ACK* and *SYN/ACK per Destination* graphs in Asymmetric mode.
- A new NTP QRM (Network Time Protocol Query Response Match) table has been added to *Dashboard > Status*.

DNS:

- DNS Rcode 1-15 is now shown in DNS Rcode Flood logs.
- DNS Profile page is re-ordered to show related features in the same section.
- DNS Profile features that cannot be used in Asymmetric mode are now hidden in the *Profile* GUI if the system is set to Asymmetric Mode.

Security Fabric:

- *Security Fabric > External Connectors*: download IP Address lists from external servers to automatically refresh Global or SPP ACLS.
- *Security Fabric > Fabric Connector* displays FortiDDoS on FortiGate Security Fabric Topology pages.

TCP/UDP Enhancements

- Added a *UDP Empty Checksum* checkbox in IP Profile, separated from *IP Strict Anomalies*. Recommended for server SPPs, not firewall SPPs.
- TCP DNS queries are now processed through all DNS feature sets, including Anomalies and TTL checks.
- *UDP Reflection Flood* logs in Symmetric Mode for inbound traffic from known reflectors without matching outbound traffic.
- *UDP Service port* field is expanded to support 256 Ports.

Foreign Packet Pause Timer for Link Events

Foreign Packet Pause timer prevents connection drops during HA failover, link failures, or reboots by pausing newly-seen connections until stability is restored.

HA System Link Failure Trigger

HA partner can now switch from Fail Closed to Fail Open mode when a system link failure occurs.

SNMP MIB updates

The following updates were made to the Simple Network Management Protocol (SNMP) Management Information Bases (MIBs):

- SNMP MIB now supports polling Global and SPP drop counts every 5 minutes.
- SNMP MIB now polls Global and SPP Attack Flags when drop counts exceed user-configured thresholds.

Daily Config Backup enhancements

Config Backup now supports scheduled backups at local times and allows on-demand or test backups to the server.

Hardware and VM support

FortiDDoS 7.0.3 supports the following hardware models:

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

FortiDDoS 7.0.3 is NOT compatible with any FortiDDoS A- / B- / E-Series hardware.

FortiDDoS Release 7.0.3 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

The following issues have been resolved in the FortiDDoS-F 7.0.3 release. For inquiries about particular bugs, please contact Fortinet Customer Service & Support.

Bug ID	Description
886093	Global ACLs configured to "Accept" (which do not drop packets and allow further processing) were previously appearing as potential drop graphs in *Drops Monitor* > *Global* > *ACL Drops*. These ACLs are no longer included in the selection list, as they do not drop any traffic.
961369	Manipulating table column configurations occasionally produces unexpected data table error messages. Refreshing the browser recovers the table.
995550	When DNS Cache is enabled in DNS Profiles for multiple SPPs, drops associated with any SPP were displayed for only one SPP.
1001821	Drops from the following attack logs were not included in *Dashboard* > *Top Attacks* > *SPP* > *Attacked HTTP Servers* table: • HTTP Method flood from source • Incomplete HTTP Request
1001822	Drops from the following attack logs were not included in *Dashboard* > *Top Attacks* > *SPP* > *Attacked DNS Servers* table. • DNS Query flood from Source • DNS Packet Track Flood from Source • DNS Exploit Anomaly: Pointer loop • DNS Query Restricted to specific domains • DNS UDP Query Blocked (Blocklisted Domains) • DNS TCP Query Blocked (Blocklisted Domains) • DNSSEC UDP Asymmetric Response Source Flood • DNSSEC UDP Asymmetric Response Flood • DNSSEC UDP Asymmetric Response Destination Flood • DNS UDP Header Anomaly: Missing Header • DNS TCP Header Anomaly: Missing Header • DNS UDP Data Anomaly - EDNS0 Multi Option Error • DNS TCP Data Anomaly - EDNS0 Multi Option Error • DNSSEC Response Type Check Mismatch • DNSSEC UDP Unsolicited Response • DNSSEC TCP Unsolicited Response • DNSSEC Deny • DNS Spoofed IP: UDP Query Flood Drop during Transparent Proxy Check • DNS Spoofed IP: UDP Question Flood Drop during Transparent Proxy Check

Bug ID	Description
	• DNS Spoofed IP: UDP Qtype All Flood Drop during Transparent Proxy Check • DNS Spoofed IP: UDP Qtype Zone Transfer Flood Drop during Transparent Proxy Check • DNS Spoofed IP: UDP Qtype MX Flood Drop during Transparent Proxy Check • DNS Header Anomaly: TCP Known Opcode • DNS UDP Query Dropped under flood (FQDN Allow list unmatched) • DNS TCP Query Dropped under flood (FQDN Allow list unmatched) • DNS Fragment Deny
1004715	No event log when a PSU failed or was powered off.
1008317	The daily config backup via sftp would fail if there were leading spaces in the server field. This was not validated at entry.
1020354	The shared secret was mistakenly required for the deletion of a cloud signaling device.
1022385	Users with full read/write access were unable to change their own or other non-globaladmin passwords or profiles. This functionality now matches documentation.
1022526	Source tracking for Protocol flood was not functioning. Note that Source Tracking is rarely triggered due to the diversity of Source IPs. Protocol rate limiting is applied when no high-rate Sources are detected.
1022565	Source tracking for UDP Port flood was not functioning. Note that Source Tracking is rarely triggered due to the diversity of Source IPs. UDP Port rate limiting is applied when no high-rate Sources are detected.
1024875 1026428 0977962	Under rare conditions during QA automation testing, certain parameters between the HA Primary and Secondary were not synchronized.
1026334	The CLI command to "boot alternate firmware" (restore alternate image) did not work correctly.
1027579	Users could run the System Recommended Threshold process from CLI without running the Traffic Statistics process first.
1027926	New KVM deployments could create a `ddosconfd` crash.
1036370	The Service Protection Policy page table may not have rendered correctly.
1038089	The system could import a security certificate created by older versions of OpenSSL but could not utilize it.
1041529	The system clock was incorrectly set when the time zone was selected as (GMT +2.0) Sarajevo, Skopje, Sofija, Vilnius, Warsaw, or Zagreb.

Bug ID	Description
1042120	Some combinations of changes to HA settings for TCP connectivity could result in failed connectivity.
1042531	From Release 7.0.1, some Scalar Thresholds showed incorrect, system maximum Estimated Thresholds instead of the calculated number which was calculated correctly.
1044169 1048778	The VM automatic 15-day trial license was not fully functional in Releases 7.0.1 and 7.0.2.
1045548	Under rare conditions, debug crashlogs could fill the log disk.
1045550	Starting from Release 7.0.1, the FortiGuard IPv6 geolocation database could exceed the FortiDDoS memory table for geolocation, leading to dataplane crashes. A temporary fix was implemented with FortiGuard, while version 7.0.3 provides a permanent solution.
1051570	Cloud signaling Shared Secret was shown in plain text during entry.
1052988	If configuring DNS Profile Domain Reputation Categories via CLI, not all categories selected were configured
1057279	Not all syslogs using TCP and Transparent settings sent.
1059658	TFTP daily config backup sometimes failed on GUI.
1061304	Memory management issues could result in dataplane restart in Release 7.0.2.
1061516	For DNS LQ Popluate, FQDNs longer than 64 characters could result in dataplane restarts, impacting traffic.
1066480	1. LQ file update information generated excessive event logs, which have now been modified to be less verbose. 2. LQ files were incorrectly categorized as "HA." They have been updated to "System" or "Health Check" as appropriate.
1072957	Several Flood drop types were not displayed in *Dashboard* > *Top Attacks* > *DNS Server* table: • DNS LQ: TCP Query flood • DNS LQ: TCP Question flood • DNS LQ: TCP Qtype All flood • DNS LQ: TCP Qtype Zone Transfer flood • DNS LQ: TCP Qtype MX flood • DNS LQ: TCP Query flood due to Negative Response
1075749	If an uploaded LQ file had invalid characters, the upload failed with no warning. The FQDN File Domain Count shows = 0.

Common Vulnerabilities and Exposures

Release 7.0.3 includes multiple precautionary upgrades of Open Source modules to ensure latest security fixes.

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

Bug ID	Description
1074482 1074483	FortiDDos Release 7.0.3 is no longer vulnerable to CVE-2024-45325

1069426	FortiDDoS is not longer susceptible to CVE-2024-3596. However, this requires that the Message-Authenticator attribute is configured in both FortiDDoS and the RADIUS server (This is common for all RADIUS users).
	From FortiDDoS CLI:
	`config system authentication radius`
	`set require-msg-auth`
	See FortiDDoS documentation for more information.
	FortiDDoS will always send the Message Authenticator attribute; however, if it does not receive a response to that attribute, it will proceed with authentication. If `require-msg-auth` is set, authentication will fail if the server does not also support this attribute.

Known issues

This section lists the known issues in FortiDDoS-F 7.0.3 release. For inquiries about particular bugs, please contact Fortinet Customer Service & Support.

Bug ID	Description
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.
1016007	Large DNS Zone Transfer responses are dropped due to the DNS Exploit Anomaly: TCP buffer underflow. DNS Zone Transfer inbound Responses are typically rare on FortiDDoS-protected DNS servers, except for backup servers. Master servers may experience outbound Zone Transfers that could result in drops, but these will not occur in Detection Mode. To maintain security, review all outbound drops in Detection Mode and disable any anomalies in the relevant DNS feature profiles. DNS and other anomalies are not DDoS vectors; they are "clean-pipe" features that can be disabled if needed.

Bug ID	Description
939713	The DNS Rcode 0 graph is not updating for response traffic related to DNS Zone Transfer queries when response packets are segmented. This typically affects outbound responses only, where Rcodes are set to the system maximum and in Detection Mode, resulting in minimal impact.
1078344	Some diagnostic commands inaccurately report the number of SPPs for VM-04 and VM-08. The correct number of configurable SPPs is 4 for VM-04 and 8 for VM-08.
995860	Facebook uses a pre-RFC standard version of QUIC, which may be dropped by FortiDDoS's QUIC version anomaly in Prevention Mode. To ensure Facebook traffic is not affected, disable this QUIC Profile anomaly on firewalls or other gateways that may handle Facebook traffic. Additionally, check outbound anomalies for each SPP for the QUIC Version Anomaly and disable the feature if detected.

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