FortiDDoS-F - Release Notes

Version 6.4.0

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/training-certification

NSE INSTITUTE
https://training.fortinet.com

FORTIGUARD CENTER
https://www.fortiguard.com

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

FEEDBACK
Email: techdoc@fortinet.com

October 5, 2022
FortiDDoS-F 6.4.0 Release Notes
00-620-730305-20221005

TABLE OF CONTENTS

Change Log

Date	Change Description
October 5, 2022	FortiDDoS-F 6.4.0 Release Notes initial release

Introduction

This Release Notes covers the new features, enhancements, resolved issues and known issues of FortiDDoS version 6.4.0 build 0406.

Before upgrading, place FortiDDoS into Bypass mode 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 upgrade is complete (GUI and all Dashboard panels are displaying):

```
Fortiddos #get system bypass status
```

`Normal` (system is inline and processing)

`Bypass` (system remains in bypass and requires manual return to inline below)

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

Ensure to clear your browser cache (or operate in incognito mode) after a firmware upgrade. The GUI is coded in JSON 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.

After upgrading from 6.1.x or 6.2.x to FortiDDoS-F 6.4.x, please check the integrity of the system Service Protection Policies (SPPs) and repair if necessary. See After upgrade on page 13 for checks to be completed post upgrade.

In early FortiDDoS-F-Series releases, the Round-Robin Databases (RRDs) were created automatically for each SPP whenever the user created a new SPP via the GUI or CLI. However, if the user makes a configuration change to the SPP while the RRD creation was in progress, then the process could be interrupted in the background. This will result in incomplete RRDs with missing information for logging and graphing of traffic and drops.

In later FortiDDoS-F-Series releases, the SPPs and RRDs for all possible SPPs are created during the upgrade process. However, existing incomplete RRDs will not be repaired. Checks of RRDs and SPPs are required if you are upgrading from 6.1.0, 6.1.4 or 6.2.0.

What's new

FortiDDoS-F 6.4.0 offers the following new features and enhancements:

New options added to the DNS profile

- Domain Reputation includes Malicious URLs, Botnet Domains and (new) Bitcoin Mining Domains.
- Options When No Cache Match now include Force TCP, Forward to Server and (new) Drop.

Enhancement to Dashboard > Status > System Information Panel

For appliances, the **Dashboard > Status > System Information Panel** now allows you to toggle the bypass ports between inline and bypass by clicking the Bypass Status information.

Enhancements to Dashboard widgets and panels

Most Dashboard widgets and panels can now be pinned to show additional information and expanded to full screen for easier viewing.

QUIC support

- New QUIC Profile which includes Anomaly checks and two handshake checks (Reflection Deny usable only with symmetric Traffic).
- New QUIC Thresholds and graphs for Initial Request, that include Request Initial packet rate Threshold, Request Initial packet per Source Threshold, and Response Initial packet rate Threshold.
- **Dashboard > Data Path Resources** now includes table occupancy for QUIC sessions.

Reports improvements

- You can now generate reports per SPP or any group of SPPs.
- Report periods now range from 1 hour to 1 year.
- You can now generate a report when a drop threshold is exceeded. The report will be for the previous 5 minutes regardless of the selected Report Period. Multiple Reports with different drop thresholds are allowed.

Enhancement DDoS Attack Log

The **Log and Report > Logs > DDoS Attack Log** has moved the Direction and SPP filters outside of the "Add Filter" menu for easier selection.

Enhancement to Anomaly Drop Graphs

The **Monitor > Drops Monitor > SPP > Anomaly Drop Graphs** now shows directionality for all graphs except for Aggregate graphs.

FORTINET-CORE-MIB and FORTINET-FORTIDDOS-MIB support

From 6.4.0 onward, the FORTINET-CORE-MIB and FORTINET-FORTIDDOS-MIB will now be included in the build and FortiCare download folders.

HTTP flow improvements

Current HTTP packets can be very long due to client cookies, resulting in truncated (segmented/fragmented) packets. FortiDDoS has now changed the way it detects HTTP flows so that Anomalies for Known Methods, Unknown Methods and Version are detected on the HTTP flow and not packet by packet. HTTP Incomplete Request Action should remain "None" since FortiDDoS cannot determine where the correct message end string is in multi-packet flows.

Enhancements to LDAPS/STARTTLS

LDAPS/STARTTLS now has additional support for CLI logins.

New CLI command: `execute restapi-restart`

The new CLI command `execute restapi-restart` is introduced to resolve reported issues of the GUI "freezing" on the login screen after a successful login.

Hardware and VM support

FortiDDoS 6.4.0 supports the following hardware models:

- FortiDDoS 200F
- FortiDDoS 1500F
- FortiDDoS 2000F

FortiDDoS 6.4.0 is NOT compatible with any FortiDDoS A- / B- / E-Series hardware.

FortiDDoS Release 6.4.0 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 6.4.0 release. For inquiries about particular bugs, please contact Fortinet Customer Service & Support.

Bug ID	Description
0810242	Resetting an SPP configuration to default, from the Service Protection > Service Protection Policy List may not reset UDP Service Ports.
0748881	TACACS+ authentication was not working for GUI logins.
0784660	If Service Protection Policy or SSL/TLS Profile used System > Address policies, the SPP Policy or SSL/TLS Profile could not be deleted until the address objects were removed.
0826613	Other Protocol Fragment Attack Log may show "Associated Port" as 65535 which is incorrect. No port information is available in most Layer 3 fragments.
0826801	TCP Zombie Flood Attack Log may show "Associated Port" as 65535 which is incorrect. There should be no port information.
0826404	Destination Flood Attack Log may show "Associated Port" as 65535 which is incorrect. There should be no port information.
0827061	Protocol Flood Attack Log may show "Associated Port" as 65535 which is incorrect. There should be no port information.
0815486	Attack logs for attack log events such as SYN/Src, SYN/Dst, Source Flood and Destination Flood, shows associated port = 0, which can be misleading. Instead, it should show "-" for these events.
0835326	When a patch file is installed, it cannot be uninstalled. Installing a patch file is a very rare occurrence, managed by the FortiDDoS dev team, so will be low impact.
0785818	Debug File, Attack Log CSV has some logs incorrectly formatted resulting in misaligned columns and some missing information.
0801906	DNS Profile, DNS Fragment option does not properly drop IPv6 DNS fragments.
0812129	If enough reports are generated to require multiple pages, the page selection buttons may not work.
0833086	Some tables may be missed in generated reports if the system has a large number of data and too many tables are requested.
0806800	Most Active Source and Most Active Destination Traffic Statistics and graphs were not accurate, erring too high compared to actual traffic.
0764676	Command `formatlogdisk` from the console does not show any output — only seen in (SSH) CLI.

Bug ID	Description
0796137	On some graphs, when no drop count has been shown for a long time and then drops occur, the system would write the graph backwards to the previous event, showing drops continuously when none actually happened (even when the logs are correct).
0812252	FDD-200F CLI `get system sensors` was not working.
0807382	After DST or Time Zone setting changed, get system status may still show the old time/zone.
0806420	After upgrade of KVM VM, it could take 10 minutes to update RRDs.
0695645	Under rare conditions, generating multiple Certificates after a restore can stop the GUI.
0804753	If SPP Layer 3 Thresholds are set to factory default via CLI, the Most Active Destination Threshold would not reset.

Common Vulnerabilities and Exposures

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

Bug ID	Description
0776398	FortiDDoS-F 6.4.0 is no longer vulnerable to the following CVE-Reference: CWE-269.

Known issues

This section lists the known issues in FortiDDoS-F 6.4.0 release. For inquiries about particular bugs, please contact Fortinet Customer Service & Support.

Bug ID	Description
0794869	If multiple feature/Profile changes are made in an SPP, the Event Logs are concatenated and become difficult to understand.
0795300	DNS Dynamic Update Queries will be dropped by DNS Query Anomaly: Query Bit Set and DNS Response Anomaly: Query Bit not Set. Enterprise user should never see Dynamic Update Queries since they are normally used by services that host large numbers of different customer domains. If in doubt, disable these 2 DNS Anomalies.
0668077	Local and External Authentication (RADIUS, LDAP, TACACS+) does not support 2-Factor Authentication.
0780476	In HA pairs, if a Primary system SPP is factory reset, the Secondary may not (reboot and) sync immediately.
0779671	HA Secondary systems may not display event logs for local events, such as logins. These can be recovered using CLI command `execute recover-eventlog`.
0693789	When FDD-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.
0686846	Online SCEP Enrollment Method of Certificate generation fails.
0638555/0637835/0634481/0633151	Multiple Queries in a single TCP DNS session (SourceIP:Port-DestinationIP:53) are allowed to exceed TCP DNS Thresholds. Fortinet's experience is that this is a very rare possibility. To work around, setting **DNS Anomaly Feature Controls: Query Anomaly: QDCount not One in Query** will drop these Queries as anomalies.
0714534	If setting Private Key and Certificate from CLI, the event log creates a blank message. Use GUI.
0750762	FortiDDoS VMs support 1024 URL Hash Indexes while others support 64,000. This is by design.
0801480	When a new SPP is created and immediately sees traffic, it may take 10 minutes (2x 5-minute cycles) before drops and other information is shown. This is architectural and will not be changed.
0783004	FQDNs with TTLs longer than 30 days will create invalid entries in the Cache.

Bug ID	Description
0795435	If DNS attack traffic is very bursty (short duration and infrequent) attack logs are correct but drop graphs may not show any information.

Upgrade notes

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
```

Upgrading to 6.3.3 causes a 15s network outage, even if FortiDDoS Fail-Open is selected for appropriate traffic ports.

To avoid this, manually enter bypass before the upgrade

```
#: execute bypass-traffic enable
```

Select "y" at the prompt

Proceed with upgrade.

The bypass will be removed automatically when the system has rebooted and is operational.

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` (Limit 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` (Limit for 200F/VM08)

`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
```
(Limit for 1500F/2000F/VM16)

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 drop 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 missing RRDs:

```
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
```