FortiDDoS-F - Release Notes

Version 6.3.1

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

April 7, 2022
FortiDDoS-F 6.3.1 Release Notes
00-620-730305-20220407

TABLE OF CONTENTS

Change Log 4

Introduction 5

What's new 6

Hardware and VM support 7

Resolved issues 8

Known issues 10

Upgrade notes 12

After upgrade 12

6.3.0 Release Notes 14

6.3.0 What's new 14

6.3.0 Resolved issues 16

6.3.0 Known issues 18

Change Log

Date	Change Description
April 7, 2022	FortiDDoS-F 6.3.1 Release Notes initial release

Introduction

This Release Notes covers the new features, enhancements, resolved issues and known issues of FortiDDoS version 6.3.1 build 0322.

Note: Firmware version 6.3.0 was removed from GA download folders because of a service-affecting bug fixed in 6.3.1. To provide information on the new features and bugs fixed in 6.3.0, the 6.3.0 Release Notes on page 14 is appended to this Release Note.

⚠ After upgrading from 6.1.x or 6.2.x to FortiDDoS-F 6.3.1, please check the integrity of the system Service Protection Policies (SPPs) and repair if necessary. See After upgrade on page 12 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 6.3.1 offers the following new features and enhancements:

Top Attacks usability improvements

Dashboard > Top Attacks header for Direction, Time Period and SPP stays visible as you scroll down the page.

Attack logs for Global ACL Rules usability improvements

The Global Deny Rule log entries in the Attack log now show the rule name in the Event Details.

Dashboard enhancements

- The Detection/Prevention Mode status of all configured Service Protection Profiles (SPPs) will now be displayed on a single panel on the Dashboard.
- Improvements have been made to the System Resources Panel.
- The Dashboard layout has been improved to enhance usability.

Hardware and VM support

FortiDDoS 6.3.1 supports the following hardware models:

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

FortiDDoS 6.3.1 is NOT compatible with any FortiDDoS A- / B- / E-Series hardware.

FortiDDoS Release 6.3.1 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 6.3.1 release. For inquiries about particular bugs, please contact Fortinet Customer Service & Support.

Bug ID	Description
0793786	Local SSL Certificate could not load via CLI.
0792773	CLI created certificate with empty content.
0791171	Blocklisted Domains uploaded or added via GUI were blocked but produced no logs nor ACL graphs.
0790526	Uploaded Blocklist IPs were blocked without Logs or Monitor ACL graphs.
0789877	Dashboard > Top Attacks > Detailed Attack Logs page header disappears when scrolling through long pages, making it difficult to understand columns.
0787761	If any condition causes the system mitigation engine to restart, Traffic Statistics become unusable and may affect traffic. This condition only happens on Release 6.3.0 which was removed from download sites for this reason.
0787743	Certain packets can cause a process restart that results in the front panel and bypass module NICs resetting with 1-2-second outages. Event logs show only that links are "up" with no "down" messages.
0786584	Dashboard > Top Attacks > Detailed Attack Logs filtering did not work.
0785925	Protection Subnets list pagination did not work, only displaying one page.
0785532	Traffic stat generation fails for UDP/ICMP/URL sometimes due to missing template files used for Traffic stats generation.
0783803	Only first fragments were added to statistics for some fragment parameters.
0783647	All content from the System > Maintenance > Offline Analysis File is included in the System > Debug File > Customer Folder. The Offline Analysis File has been removed.
0780493/0776987	KVM-based VM on upgrade will not automatically repair partial or missing RRDs affecting graphs and logs.
0779339	In an HA Pair, adding a DNS profile with some options in the primary is not fully synchronized with the secondary. The Secondary then reboots to obtain the full configuration from the Primary.
0776121	Allowed users could change their password via the admin menu pull-down but the system did not force a logout for that user, which is industry standard. User will be logged-out after change and must login with the new password.
0776057	Read-only users could complete the password change process from the admin drop-down menu but the password would not change and no warning was included that only write-allowed users can change their own passwords.

Bug ID	Description
0774600	Interface filter could not filter for all configuration state possibilities.
0630479	If multiple changes are made on a GUI page before saving, an event log is created for only one change.

Common Vulnerabilities and Exposures

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

Bug ID	Description
0784333/0776312/0772170	FortiDDoS-F 6.3.1 is no longer vulnerable to the following CVE/CWE-References: CWE-120, CWE-121, CWE 325.
0772198	FortiDDoS-F 6.3.1 is no longer vulnerable to the following CVE/CWE-References: CVE-2021-36173.

Known issues

This section lists the known issues in FortiDDoS-F 6.3.1 release. For inquiries about particular bugs, please contact Fortinet Customer Service & Support.

Bug ID	Description
0796137	On some graphs, when no drop count has been shown for a long time, if drops occur the system writes the graph backwards to the previous event, showing drops continuously when none actually happened (the logs are correct).
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.
0794869	If multiple feature/Profile changes are made in an SPP, the Event Logs are concatenated and become difficult to understand.
0785818	In Debug download > Customer Folder, the Attack log CSV does not always parse the attack log detail into correct columns.
0783803	Second and subsequent UDP fragments to Port 53 are not shown on statistics graphs.
0780476	In HA pairs, if a Primary system SPP is factory reset, the Secondary may not (reboot and) sync immediately.
0779671	HA Secondary systems do not create event logs for local events, such as logins.
0765443	FortiDDoS will drop segmented/fragmented HTTP packets if HTTP Profile > Version Anomaly is enabled. **Do not enable** HTTP Version Anomaly. GET Cookies can be very large and frequently result in segmented HTTP packets. Trust the Method Thresholds to find HTTP attacks.
0764676	`formatlogdisk` command from console does not show any output - only seen in (SSH) CLI.
0750762	FortiDDoS VMs support 1024 URL Hash Indexes while others support 64,000. This is by design.
0714534	If setting Private Key and Certificate from CLI, the event log creates a blank message. Use GUI.
0695645	Under rare conditions, generating multiple Certificates after a configuration restore can stop the GUI.
0693789	When FDD-VM is operating on a virtual machine with underlying hardware supporting SR-IOV, disabling ports leads to unexpected results.

Bug ID	Description
0686846	Online SCEP Enrollment Method of Certificate generation fails.
0678445	Purging a large number of ACLs from an SPP can take more than 30 seconds with no progress indication.
0678434/0678433	FortiDDoS-F 6.1.x, 6.2.x and 6.3.x do not support LDAPS/STARTTLS.
0676634	GUI will allow multiple and overlapping Hash entries various HTTP Thresholds like URL, Host, etc. Use care when manually entering indexes.
0668077	Local and External Authentication (RADIUS, LDAP, TACACS+) does not support 2-Factor Authentication.
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.

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
```

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
```

6.3.0 Release Notes

This Release Notes covers the new features, enhancements, resolved issues and known issues of FortiDDoS version 6.3.0 build 0314.

Note: Firmware version 6.3.0 was removed from GA download folders because of a service-affecting bug fixed in 6.3.1. To provide information on the new features and bugs fixed in 6.3.0, this Release Note is appended to the 6.3.1 Release Note.

6.3.0 What's new

FortiDDoS-F 6.3.0 offers the following new features and enhancements:

DNS Profile enhancements

- Added FQDN Allow/Blocklist file upload, manual entry, and regex entries.
- FortiDDoS-F now supports DNS "0x20" mixed case FQDNs.

New DNS Header Anomaly

Incomplete DNS can now be used to block non-DNS traffic to Port 53.

DNSSEC enhancements

FortiDDoS-F has added DNSSEC inspection, anomaly and mitigation options.

UDP Service Ports monitor

User-entered UDP Service Ports over 9999 are now monitored for possible reflection floods.

New graphs and tables on FortiGate Security Fabric Dashboard

FortiDDoS-F now supports the following graphs and tables on FortiGate Security Fabric Dashboard: System Information, Data Path Resources, Aggregate Drops and Top Attacks.

SSL/TLS traffic inspection

FortiDDoS-F 1500F can now inspect SSL/TLS traffic for all HTTP Anomalies and Thresholds. Proper SSL Certificates are required.

Note: This is experimental in 6.3.0 and performance has not been confirmed.

LDAP, RADIUS, TACACS+ remote password authentication

LDAP, RADIUS, TACACS+ remote password authentication is now available with local username, profile and trusted hosts settings. This now supports GUI, CLI and Console logins.

TCP Profile enhancement

TCP Profile now adds Foreign Packet Threshold when Foreign Packet Validation is enabled.

New IP Reputation options

Added Phishing, Spam and TOR (exit nodes) Categories to IP Reputation options.

Debug enhancements

- Debug file now has CUSTOMER folder which includes: Config, Attack logs, Thresholds, Protection Subnets list (event log in MySQL format to be improved in a later release). Do not use Offline Analysis file.
- Additional debug logs are added for SNMP.

Packet Capture enhancements

Additional packet capture options are now available.

System time change in Event Log

An Event Log is now added when admin changes system time.

Out of Memory (OOM) conditions

Out of Memory (OOM) conditions are optionally set to pass traffic (bypass - default) or block packets. Please see documentation for conditions that may result in OOM drops.

New RRD troubleshooting and repair CLI commands

Additional RRD troubleshooting and repair CLI commands are now available.

```
execute create-spp-rrd spp_id 15 among others
```

```
check_stale_rrd_files
```

New User (admin) options

Additional menu items added to the User (admin) drop-down in the GUI:

- System: Reboot / Shutdown
- Configuration Backup / Restore
- Change Password

GUI enhancements

- Additional special characters are allowed for admin users: `a-Z -9_.-*@`.
- Data Port Speed and Duplex settings are shown on Network > Interface page.
- Global ACL names are included in graphs.
- Enabled/Disabled status of Global and SPP ACLs is displayed in ACL lists.
- Variable column widths and text wrapping is added to Dashboard > Status > Top Attacks panel, for improved readability of attack events.

- Link speed addition to Network GUI.
- Bypass status icon and inline/bypass text is added to the Dashboard > Status > System Information panel.
- Filter conditions for several parameter lists (ACLs, Network Ports, etc.) are improved.
- Network > Interface list can be filtered by Link Status and Config Status (for Port-Pairs and Ports).
- Improved GUI for System >SNMP > v1/v2/v3.
- A spinning "loading" icon is shown when the system is building list pages, such as Attack Logs.
- For most column based lists, clicking the settings (⚙) icon in the list header allows the user to customize the columns shown.
- Dashboard > SPP adds a column for SPP Status (Enable/Disabled).

6.3.0 Resolved issues

The following issues have been resolved in the FortiDDoS-F 6.3.0 release. For inquiries about particular bugs, please contact Fortinet Customer Service & Support.

Bug ID	Description
0779660	In the rate circumstance where a system was rebooted in the middle of collecting traffic statistics the collection was not aborted correctly and would prevent future traffic statistics collection.
0778284	In HA pair, if the Secondary system is rebooted, Mgmt1 port reverts to earlier IP address.
0777916	Execute shutdown from GUI or CLI did not fully power-down the system.
0774630	In Asymmetric Mode, inbound SYN-ACK packets are graphed but inbound SYN packets are also graphed. Change is made to show matching outbound "virtual" SYNs for clarity.
0771321	When restoring a configuration, RRDs may not be reset correctly resulting in some graphs showing data.
0770084	In some conditions where an SSL server requires verification of the client certificate, SSL/TLS Profile Protocol Anomaly or Version Anomaly would drop the packets, preventing connection.
0768844	If the configuration was restored on a system running live traffic, interface states may be set to "down" requiring manual intervention to bring them up.
0766911	Monitor > Layer 3/4/7 > Layer 3 > Other > Fragmented Packets graph did not display UDP Fragments.
0756613	If a user has more than 10 Service Protection Policies configured (1500F) SNMP MIB Queries become intermittent.
0756558	Blocking DTLS Server Hello per Destination may block all traffic to the Destination (protected) IP address.

Bug ID	Description
0754792	After creating Private Data Encryption key in System > Admin > Setting, other non-secure parameters on the page cannot be changed without re-entering the key.
0753190	Most Active Source graph was updated in both directions when DNS Query traffic was only sent in one direction.
0749266	TCP Session graph (Traffic Monitor -> Layer3/4/7, Select SPP, Select Layer 4-> Other tab, TCP session graph) was not displaying 1/2-open sessions.
0748374	If an SPP that had traffic/graphs/drops was deleted, some logs may not have been deleted, resulting in logs with no SPP identifiers.
0748296	If user attempted to create more than 64 DNS Profiles via CLI, the error message included extraneous information.
0747439	When restoring config via GUI, the API was not waiting until restore was complete before allowing a login, with unexpected results.
0747082	Possible UDP Reflection Flood event is not included as data shown for Dasboard > Top Attacks > SPP > Top attacked UDP Ports.
0741379	SSL/TLS Version Anomaly was only checked for Content Type 22 messages.
0736263	When Packet Capture result was an empty file, it could not be opened, giving a format error. The empty file can now be opened, showing no captured packets.
0736013	Backup and restore from the GUI could result in missing SPPs.
0726191	DTLS UDP service ports are excluded from System Recommendation Port thresholds. Ensure DTLS profile is configured for SPPs with DTLS service ports.
0672585	Invalid DNS packets could be dropped even when no DNS Anomalies were enabled with no logging. FortiDDoS will now drop and log as DNS UDP Header Anomaly: Missing Header. This is a fixed anomaly with no disable option.
0672585	Invalid DNS packets could be dropped even when no DNS Anomalies were enabled with no logging. DNS Header Anomaly "Incomplete DNS" (default off) is added to control this check.
0626478	Admin > Administator accounts now support Trusted Hosts after external password authentication by LDAP / RADIUS / TACACS+.

Common Vulnerabilities and Exposures

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

Bug ID	Description
0744346	FortiDDoS-F 6.3.0 is no longer vulnerable to the following CVE/CWE-References: CVE-2021-3711, CVE-2021-3712, CWE-788.

6.3.0 Known issues

This section lists the known issues in FortiDDoS-F 6.3.0 release. For inquiries about particular bugs, please contact Fortinet Customer Service & Support.

Bug ID	Description
0783803	Second and subsequent UDP fragments to Port 53 are not shown on statistics graphs.
0780476	In HA pairs, if a Primary system SPP is factory reset, the Secondary may not synchronize immediately.
0779671	HA Secondary systems do not create event logs for local events, such as logins.
0750762	FortiDDoS-F VMs support 1024 URL Hash Indexes while others support 64,000. This is by design.
0714534	If setting Private Key and Certificate from CLI, the event log creates a blank message. Use GUI instead.
0695645	Under rare conditions, generating multiple Certificates after a configuration restore can stop the GUI.
0693789	When FDD-VM is operating on a virtual machine with underlying hardware supporting SR-IOV, disabling ports leads to unexpected results.
0686846	Online SCEP Enrollment Method of Certificate generation fails.
0678445	Purging a large number of ACLs from an SPP can take more than 30 seconds with no progress indication.
0678434/0678433	Releases 6.1.x, 6.2.x and 6.3.0 do not support LDAPS/STARTTLS.
0676634	GUI will allow multiple and overlapping Hash entries of various HTTP Thresholds like URL, Host, etc. Use care when manually entering indexes.
0668077	External Authentication (RADIUS, LDAP, TACACS+) does not support Two-Factor Authentication.
0638555/0637835/0633151	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.
0630479	If multiple changes are made on a GUI page before saving, an event log is created for only 1 change.