Release Notes

FortiDDoS-F 8.0.0

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

April 23, 2026
FortiDDoS-F 8.0.0 Release Notes

TABLE OF CONTENTS

Change Log

Date	Change Description
April 23, 2026	FortiDDoS-F 8.0.0 Release Notes initial release

Introduction

This Release Notes covers the new features, enhancements, resolved issues and known issues of FortiDDoS version 8.0.0 build 0007.

Special Notes

FortiDDoS F-series Release 8.0.0 is a direct, one-step upgrade from any previous FortiDDoS release. No intermediate steps are required.

- If you are using DNS LQ Populate, before upgrade, go to *Global Protection* > *DNS LQ Populate* > *Valid FQDN* table and Search for the asterisk character "*". If this returns FQDNs, after upgrade, go to *Global Protection* > *DNS LQ Populate* and disable *FQDN Check* which is enabled by default starting 7.2.2.
- FQDN Check checks for illegal characters (any character other than "-" or "_") in FQDNs and does not add those FQDNs to the table. However, Fortinet is seeing FQDNs including "*" in the actual FQDN, not just as a wildcard indicator in the domain definition. Bind9 DNS servers (at least) accept these and provide good responses. If those are present, *FQDN Check* must be disabled.

GUI changes on upgrade from releases below 7.0.1

- In Release 7.2.1, IP Profiles > UDP Empty Checksum Check is disabled by default. If it was previously enabled in a lower release, it will also be disabled during the upgrade, changing your configuration. The only SPPs that require this feature to be disabled are those using IPsec NAT Traversal.

  If upgrading from Release 7.0.3 or higher, review all IP Profiles and note which ones had this feature enabled. After the upgrade, re-enable the feature for those Profiles.

  UDP Empty Checksum Check helps stop scans for known UDP reflection ports but can block IPsec NAT Traversal traffic (IPsec over UDP 4500).
- GUI access via TLS 1.1 will be disabled after upgrade to 7.0.1 or higher as a security improvement. The option can be re-enabled by the user if desired.
- On upgrade to 7.0.1 or higher, 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.
- Renamed licensing labels on *System* and *Dashboard* pages for improved clarity.

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.

FortiGate Transition from client SSLVPN to IPSec

FortiGate systems will be transitioning away from SSLVPN in newer releases. If FortiDDoS has not seen IPsec or has seen only site-to-site VPN traffic, **VPN Thresholds may be too low.**

Ensure you understand the transition with the firewall team and that Thresholds for:

- Protocol 50 (ESP/IPsec),
- UDP 4500 (IPsec NAT Traversal) (sometimes UDP 4501 for non-FortiGate VPNs) and
- UDP 500 (IKE)

are adequate. Too-low Thresholds will block VPN traffic.

If unsure, contact Fortinet Support.

What's new

FortiDDoS-F 8.0.0 offers the following new features and enhancements:

- The *Allow Inbound SYN-ACK* setting is moved from *Global Protection* > *Deployment* to the *TCP Profile* applied to the SPP. If SPPs expect only inbound sessions, like web servers, this option can be disabled so that all inbound SYN-ACKs are dropped. Otherwise, we suggest enabling this option on all TCP Profiles.
- The *System* > *Settings* menu has been moved to the main menu list from *System* > *Admin* > *Settings* tab.
- The following *Per-Destination Thresholds* are now available. These are ideal for use in large, mixed-use SPPs in ISP-like environments.
  - ESP (Proto 50) per Destination
  - UDP Source port 53 per Destination
- *System Recommendations* now creates *Rcode:0* and *Rcodes:1-15* Threshold ranges.
- The *DNS Query TKEY* Threshold is now available.
- The *System Recommended Thresholds* setting has been improved to reduce false positives on popular UDP applications such as Microsoft Teams and Zoom. These changes are applied automatically when new *System Recommended Thresholds* are created.
- *System Recommendations* now generates three TCP port ranges: 0–442, 4444–10239, and 10240–65535. Since TCP ports are not common DDoS vectors, ports such as 8443 and other API ports may raise the full-range threshold, which is expected behavior.
- Admin users with *super_admin_profile* can now create their own dashboard views that are persisitent during any session and between sessions.
- FortiDDoS-F supports an optional (default disabled) and customizable pre-login warning banner. This message can be customized via *System* > *Replacement Messages*.
- FortiDDoS-F now sends attack telemetry data to FortiGuard. This will assist Fortinet to improve the product and reporting. Users can opt-out from sending this data.
- An option has been added to create an inbound SYN service ACL per SPP. When an SPP contains only services that never expect inbound SYN packets — such as firewall NAT pools, Wi-Fi gateways, and outbound proxies — this ACL drops all inbound SYN packets without requiring thresholds.
- System mail server access settings have been moved from the *Log & Report* > *Alert Mail Settings* > *Mail Server* tab to the *System* > *Maintenance* > *Mail Server* tab. Other Alert Mail event log settings remain in *Log & Report* > *Alert Mail Settings*.
- A *Custom Monitor* option has been added under the *Monitor* menu, allowing frequently used Monitor 3/4/7 graphs of any type to be consolidated into a single, customizable page.
- The *DNS Profile* page now features collapsible sections for easier navigation.
- The Report Browse page now displays pie and bar graphs for the following:
  - Attack Types Distribution (pie)
  - Attacks per Destination (Protected IP) (bar)
  - Flood Events Distribution (pie)
  - ACL Events Distribution (pie)
  - Anomaly Events Distribution (pie).

  Individual chart entries can be toggled off for a clearer view of the remaining data. Note that these charts are available in the GUI only and are not included in PDF or Word reports.
- Graph Y-axes now support Logarithmic (base 2) labels.

- An *SNMP Trap with Threshold* is added for *Data Path Resources*.
- The firmware file drag-and-drop under *System* > *Firmware* has been replaced with a file selector.
- Debug files now include a CSV file of all customer-configured ACLs, IPv4 Blocklisted file and external resource files.

Hardware and VM support

FortiDDoS 8.0.0 supports the following hardware models:

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

FortiDDoS 8.0.0 is NOT compatible with any FortiDDoS A- / B- / E-Series hardware.

FortiDDoS Release 8.0.0 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 8.0.0 release. For inquiries about particular bugs, please contact Fortinet Customer Service & Support.

Bug ID	Description
1212811	Source Port (53) is now shown in UDP Unsolicited Response logs for clarity.
1215041	The default time for Report Schedule Type Daily displayed as "0" (00:00), which was not accepted by the GUI or CLI. The default time has been corrected to "1" (01:00).
1220784	Downloaded event log files now correctly reflect any applied filters, rather than returning all logs.
1227372	Entering an FQDN string in the FQDN/Hash Index field of the FQDN graph no longer returns a "no data" response.
1239579	Flowspec scripts containing an ACL for UDP Source Port 53 per destination incorrectly blocked the destination port instead of the source port.
1243419	VM users were unable to add a new license after a previous license (typically a trial) expired. The GUI page did not display a file upload section, and the GUI CLI did not function as expected. Both methods now work correctly.
1245458	Graph headers and titles restored for: • *Monitor 3/4/7 > TRAFFIC MONITOR > SPP: SPP* graph • *Monitor 3/4/7 > TRAFFIC MONITOR > Subnets: Subnets* graph
1251768	Read-only users were incorrectly able to perform the following actions: reboot the system, boot alternate firmware under *System > Firmware*, change the time zone under *System > Maintenance*, start, stop, and download packet captures, and start/stop debug trace under *Network > Diagnostics*.
1252442	Drops from IPv6 Global ACLs now display the ACL name.
1255648	FDD-3000G no longer continues to send logs to FortiAnalyzer after configuration is removed.
1266168	Upgrade to 7.2.x resulted in *DROPS MONITOR > SPP > Aggregate > Flood Drops > Layer 4 Graph > SYN/ACK* drop subgraph data copied to the new UDP Destination Port 53 per Destination subgraph. Round-Robin-Database objects were re-used in error. This is fixed in 8.0.0 but UDP Destination Port 53 per Destination graph will be reset to 0 and filled going forward with correct data.
1275323	The following log events were either missing from the *Dashboard > SPP > Attacks* table or lacked detailed information: • DNS FQDN Flood • DNS Rcode 0 Packet Per Destination Flood • DNS TCP Query Packet Per Destination Flood • DNS LQ: TCP Query Packet Per Destination Flood

Common Vulnerabilities and Exposures

Release 8.0.0 contains precautionary upgrades to various common source modules.

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

Bug ID	Description
N/A	Added precautionary upgrades of several open source modules for improved security.

Known issues

This section lists the known issues in FortiDDoS-F 8.0.0 release. For inquiries about particular bugs, please contact Fortinet Customer Service & Support.

Bug ID	Description
1181791	DNS Rcode egress rates may show as very slightly (single digits) higher than ingress rates, when there are no dropped packets. This is a design limitation and will not be fixed.
1215041	Daily (Last 24 Hours) reports cannot be run at midnight (00:00-23:59). They must be run from 1:00am (01:00-00:59).
1281045	If Drop Monitor - Global - ACL Drops - DACL/ADACL Rule Drops graph (available only on 3000F/G with ADACLs enabled) is added to the *Custom Monitor* page, it displays with missing options, labels and data. Use the normal drops graph.
1280185	Customers running Release 7.2.3 may experience continuous Attack Log purge event log messages occurring every five minutes.
1217532	When a user logs out and logs in with a different administrative username, the previous username may still show. A page refresh corrects the username info.
1212805	Foreign Packets (Aggressive Aging and Slow connections) drop logs may show Source Port instead of Protected Port.
1152256	Outage times during inline-to-bypass and bypass-to-inline transitions caused by dataplane crashes have been reduced. **Note:** FortiDDoS does not support hitless transitions. For sensitive traffic or BGP use cases, an external bypass bridge is recommended. Fortinet has had positive experience with the Niagara Networks 3808, which offers fast transitions through heartbeat detection and electrical bypass.
1148285	When changing REST-API Admin password, it is displayed in clear text in event log.
1135116	Dashbaord > System Resources expanded timeline graphs may occasionally show Month/Day-of-month (Jul 27) instead of Day/Day-of-month (Sun 27).
1016007	Large DNS Zone Transfer responses may be dropped due to the DNS Exploit Anomaly: TCP Buffer Underflow. This typically affects inbound responses on backup DNS servers protected by FortiDDoS. Master servers may show outbound Zone Transfer drops, but these are not dropped in Detection Mode. To avoid unintended impact, review outbound drops in Detection Mode and disable any triggered anomalies in the corresponding DNS feature profiles. DNS and other anomalies are not DDoS vectors—they are clean-pipe features and can be safely disabled if needed.

Bug ID	Description
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.
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.
918768 923612 924121	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.
882029	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.
693789	When FortiDDoS-VM is operating on a virtual machine with underlying hardware supporting SR-IOV, disabling ports leads to unexpected results.
678445	Purging a large number of ACLs from an SPP can take more than 30 seconds with no progress indication.

Upgrade notes

FortiDDoS F-series Release 8.0.0 is a direct, one-step upgrade from any previous FortiDDoS release. No intermediate steps are required.

Special Notes

- If you are using DNS LQ Populate, before upgrade, go to *Global Protection* > *DNS LQ Populate* > *Valid FQDN* table and Search for the asterisk character "*". If this returns FQDNs, after upgrade, go to *Global Protection* > *DNS LQ Populate* and disable *FQDN Check* which is enabled by default starting 7.2.2.
- FQDN Check checks for illegal characters (any character other than "-" or "_") in FQDNs and does not add those FQDNs to the table. However, Fortinet is seeing FQDNs including "*" in the actual FQDN, not just as a wildcard indicator in the domain definition. Bind9 DNS servers (at least) accept these and provide good responses. If those are present, *FQDN Check* must be disabled.

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.

When upgrading, place all Service protection Policies (SPPs) into Detection Mode. After upgrading, review *Dashboard* > *Top Attacks* for the 1-hour period, for all SPPs. If unusual drop events are noted, or you are unsure, contact FortiCare support for review.

HA Systems

Each system must be upgraded separately, and traffic will briefly be interrupted even when Fail-Open systems or Traffic Bypass are enabled.

Pause HA from the Primary system (*System* > *High Availability*), which breaks the HA connection but preserves HA settings.

1. Divert traffic away from the Primary system and upgrade the Primary first.
2. After the upgrade completes, return traffic to the Primary.
3. Upgrade the Secondary system.
4. On the Primary, select *Unpause* under *System* > *High Availability*.
5. After rejoining HA, the Secondary may reload its configuration, causing a brief traffic interruption.

For further info, see the Handbook.

www.fortinet.com