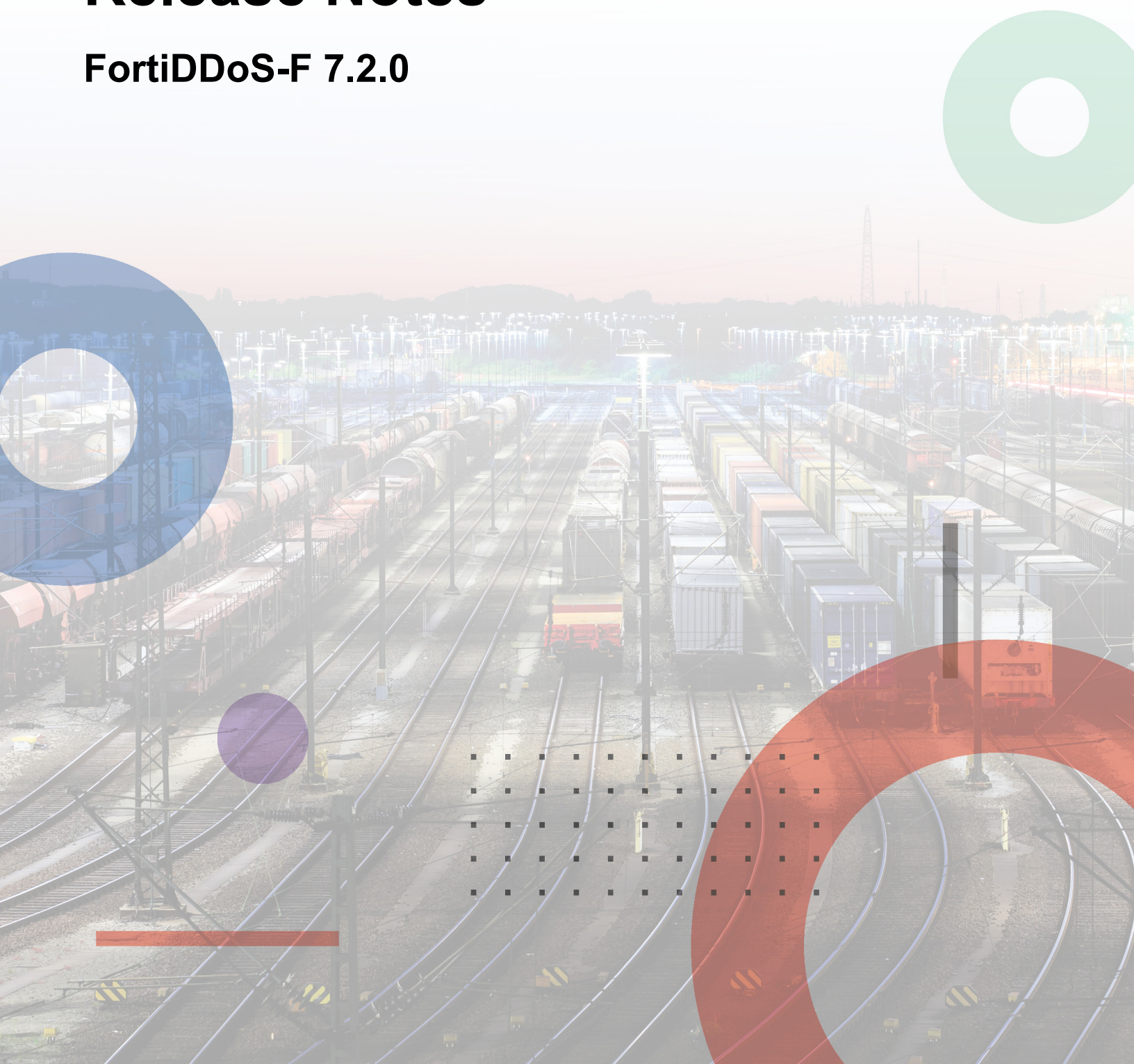
Release Notes

FortiDDoS-F 7.2.0



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

June 17, 2025
FortiDDoS-F 7.2.0 Release Notes

TABLE OF CONTENTS

Change Log

Date	Change Description
June 17, 2025	FortiDDoS-F 7.2.0 Release Notes initial release

Introduction

This Release Notes covers the new features, enhancements, resolved issues and known issues of FortiDDoS version 7.2.0 build 0804.

Special Notes

FortiDDoS F-Series Release 7.2.0 is the next release after 7.0.5. It is a direct, one-step upgrade from any previous FortiDDoS release. No intermediate steps are required.

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 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.

Manual traffic bypass may 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, for earlier hardware versions. Please see the 7.2.0 handbook for information or use the workaround below to force bypass.

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-F 7.2.0 offers the following new features and enhancements:

- You can now change *SPP Membership* from the *Protection Subnets List*.
- You can now link directly to the SPP shown in the *Protection Subnets List*.
- You can now pause HA while upgrading and preserve the HA settings.
- *SPP Traffic Statistics* now show statistics based on *Peak traffic* and *95th Percentile traffic*. 95th Percentile removes the top 5% of all traffic peaks which can be effective at removing attacks that occur during learning periods.
- The *Network* > *Interface* > *Traffic Ports* list now shows the *Link Down Sync* setting for each port pair.
- The *Dashboard* > *Status* > *System Resources* table now supports mgmt CPU as well as existing Data-plane CPU usage indicators. The system will also generate an event log if the mgmt CPU exceeds 90% load for longer than 5 minutes. High-rate spikes are not unusual since the CPU will spike when making changes.
- You can now adjust the *TCP/UDP Port Low Traffic Threshold* to reduce the number of port ranges without affecting other *System Recommended Thresholds*.

  Previously, adjusting Port Thresholds required either manual changes per port or re-running System Recommendations—both of which would overwrite existing custom settings. These adjustments are especially useful, as *TCP/UDP Port and Scalar Thresholds* are the most commonly modified after applying recommendations.
- FortiDDoS-F now supports IP-in-IP tunneling attack detection, configurable under *Service Protection Policy* > *IP Profile*, these drops will be reported as IP Tunneling Attacks.
- FortiDDoS-F now drops un-ratified L3 Protocols as part of *IP Profile* > *IP Strict Anomalies*.
- Improved Event Logs for User and System-Driven Bypass Actions.
- If IPv4 and IPv6 geolocation databases are not used, the *GEO Update Status* option on the FortiGuard page can be disabled to prevent their download. This setting applies to both databases simultaneously.
- Improved event logs for *Power Supply* failures.
- Full debug files now include additional details for *Bypass Status*, *Transceiver Status*, and *Dataplane Interface Hardware* diagnostics.
- Outage durations during inline-to-bypass and bypass-to-inline transitions caused by dataplane crashes have been reduced.

  Note: FortiDDoS-F bypass design does not support “hitless” transitions. For sensitive traffic or BGP environments, Fortinet recommends using an external bypass bridge, such as the Niagara Networks 3808. Its heartbeat detection and electrical bypass features enable faster transitions.
- The *Dashboard* > *Status* > *System Information* > *Bypass Status* link icon now turns RED in bypass mode for improved visibility.
- The *Debug Files* page now supports selecting and deleting multiple items simultaneously.
- From Monitor 3/4/7 graphs under Layer 7 > DNS, you can now access *Scalar Threshold* pages for:
  - DNS Query UDP
  - Question Count UDP
  - Fragment UDP
  - QType MX UDP
  - QType All UDP
- System Debug files now use improved compression for reduced size.

- To improve accuracy and include Management CPU metrics in *Dashboard* > *System Resources*, existing Data Plane (DP) CPU data had to be cleared.

Hardware and VM support

FortiDDoS 7.2.0 supports the following hardware models:

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

FortiDDoS 7.2.0 is NOT compatible with any FortiDDoS A- / B- / E-Series hardware.

FortiDDoS Release 7.2.0 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 7.2.0 release. For inquiries about particular bugs, please contact Fortinet Customer Service & Support.

Bug ID	Description
1100311	When IP Reputation or Domain Reputation Subscriptions expire, FortiDDoS now removes these databases to prevent false-positive drops caused by the database aging with no updates.
1110826	Using default, outdated IP and Domain Reputation databases without a subscription caused false positives when categories were added to IP or DNS Profiles. Matching IPs were dropped in Prevention Mode.
1111076	Timezone for Türkiye corrected to reflect no Daylight Saving Time (DST).
1118483	GUI implied that a user could append/prepend password characters in the SNMPv3 Authentication and Private Password fields, but only the added characters were used. Full password entry is now required.
1118829	The graph for *System Generated Packet* may not have displayed correctly for all SPPs.
1129087	200F/1500F systems CLI: set power-off-bypass-mode fail-open/fail-closed may have shown an error.
1132435	When a manual *Report Purge* was peeformed, the system would continue to purge all new *Reports*.
1132704	Non-admin users were able to upload traffic statistics files from other systems.
1133035	For external connectors, when HTTP Basic Authentication is disabled, username/password fields are now hidden to avoid confusion.
1138994	Loss of Signal on LAN-side (odd-numbered) ports in Wire Mode did not disable Tx on the corresponding WAN-side interface.
1140997	1. In some cases, setting NTP via the GUI failed, causing the system time to be set several months behind. 2. NTP servers using Kiss of Death (KoD) could block FortiDDoS NTP queries.
1141643	If the total number of *Protected Subnets* is greater than 250, the *Protection Subnets List* would not display.
1144092	IInbound ingress traffic with VLAN headers was double-counted in *Dashboard* Interfaces and *Traffic Monitor* > *Interface* graphs. This was a display issue only; SPP traffic and mitigation were unaffected.
1150270	The Thresholds page will now display the Period Used, algorithm used (Peak or 95th percentile), date and time crated. This will only show for System Recommendations requested after the upgrade to 7.2.0.

Bug ID	Description
1152047	IPv6 attack logs were not sending SNMP Traps, even when configured.
1152626	SNMP Trap configurations remained in the system after deletion.
1155249	TCP session idle timer differences between FortiDDoS and syslog servers may have caused lost logs.
1159363	CLI command `get system sensor` did not display Power Supply temperatures for FDD-2000F.
1163928	The download of a generated security certificate might have displayed the extension as ".cer" instead of ".csr"
1166039	The CSV option appeared twice on Event Log Remote configuration page.
1133603 1133598	External Resource selection was unavailable when configuring IPv6 Global or SPP ACLs.
N/A	System Debug files were not compressed, despite the .zip file type.

Common Vulnerabilities and Exposures

Release 7.2.0 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 7.2.0 release. For inquiries about particular bugs, please contact Fortinet Customer Service & Support.

Bug ID	Description
678445	Purging a large number of ACLs from an SPP can take more than 30 seconds with no progress indication.
1151549 904954	Global and SPP ACL entries can be repositioned in the GUI, but each action only moves the entry one row at a time. For moving entries multiple rows, refer to the handbook for CLI script guidance.
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.
1151658	During a dataplane restart, the system enters bypass mode, but Port Down event logs are not generated due to the dataplane being unavailable. This behavior is architectural and cannot be changed.
1170964	CLI: get system sensors does not report PSU info for 1500F/1500F-LR.
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.
678445	Purging a large number of ACLs from an SPP can take more than 30 seconds with no progress indication.
693789	When FortiDDoS-VM is operating on a virtual machine with underlying hardware supporting SR-IOV, disabling ports leads to unexpected results.
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.
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.
942816	FortiDDoS VM manual force FortiGuard update will not work. There is a workaround via shell which will be documented.

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.
1011488	DNS Known Opcode Anomalies are shown as DNS Header Anomaly drops. This is design Intent and won't be changed. It is documented from the 7.0.1 Handbook.
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.
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.
1089205	For Windows 11 Pro with some Firefox browser versions, Dashboard > Top Attacks > Summary page links to SPPs may not display or work. Use Chrome or Edge if possible. Windows 10 Pro works with all 3 browsers. Since most FF versions work, this will not be fixed. Upgrade FF version.
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.

Upgrade notes

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.

www.fortinet.com