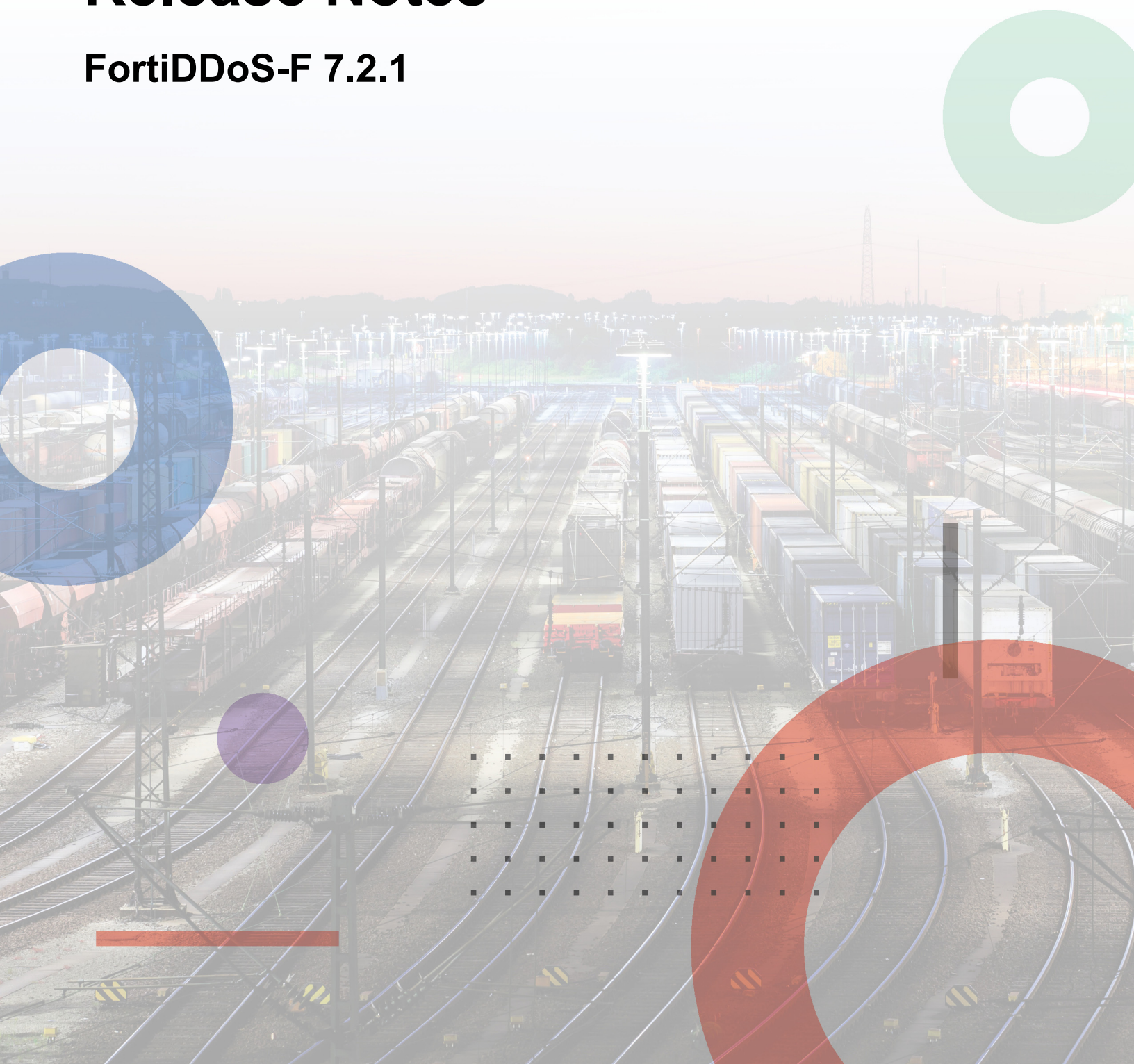
Release Notes

FortiDDoS-F 7.2.1



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

August 26, 2025
FortiDDoS-F 7.2.1 Release Notes

TABLE OF CONTENTS

Change Log

Date	Change Description
August 26, 2025	FortiDDoS-F 7.2.1 Release Notes initial release

Introduction

This Release Notes covers the new features, enhancements, resolved issues and known issues of FortiDDoS version 7.2.1 build 0818.

Special Notes

Upgrade any FortiDDoS F-Series firmware Release directly to 7.2.1. No intermediate steps are required.

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.

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.

FortiGate Transition from client SSLVN 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 7.2.1 offers the following new features and enhancements:

- IP Profile UDP Empty Checksum Check is now disabled by default in Release 7.2.1. When upgrading from a release below 7.2.1, it will also be disabled in all IP Profiles. Please review its use in all SPPs.

  SPPs using IPsec NAT Traversal must keep this option disabled. For most other SPPs, the option can be safely enabled. It is useful for blocking constant scans of known UDP reflection ports.
- Added an ACK=0 check for SYN packets in TCP Strict Anomalies. According to the TCP RFC, SYN packets should not contain an ACK number because they are the first packet in a connection.

Hardware and VM support

FortiDDoS 7.2.1 supports the following hardware models:

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

FortiDDoS 7.2.1 is NOT compatible with any FortiDDoS A- / B- / E-Series hardware.

FortiDDoS Release 7.2.1 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 7.2.1 release. For inquiries about particular bugs, please contact Fortinet Customer Service & Support.

Bug ID	Description
1175004	Two factor Authentication entry field did not always show on GUI login page.
1156568	Concurrent Connections per Source flood drops were reported without threshold being exceeded.
1168538	ACL tables were sometimes missing from pdf downloads from *Dashboard* > *Top Attacks* > *SPP* pages.
1167625	Global ACL rules could not be re-ordered more than one step at a time. Rules can now be reordered throughout the rules list.
1182268	*DTLS Profile* > *Protocol Check* did not drop all DTLS Protocol anomalies.
1189232	The header bar did not always display the hostname after login, until a browser refresh. Note, starting version 7.2.1 onwards, only the hostname is displayed, not the Model.
1170964	CLI: "get system sensors" did not return PSU information for FDD-1500F/1500F-LR.
1175300	Authentication 2-factor token was not working for RADIUS.
1167728	Renamed licensing labels on *System* and *Dashboard* pages for improved clarity.

Common Vulnerabilities and Exposures

Release 7.2.1 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 7.2.1 release. For inquiries about particular bugs, please contact Fortinet Customer Service & Support.

Bug ID	Description
1195255	When upgrading from 7.0.3 to 7.2.1, the system may generate a bogus printout stating "upgrade path not found," even though the upgrade completes successfully.
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.
1176560	SNMP Trap Receivers may fail with SNMPv3 authentication. This issue may be related to passphrases containing special characters.
678445	Purging a large number of ACLs from an SPP can take more than 30 seconds with no progress indication.
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.
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.
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.
1179746	Downloading a PDF from *Dashboard* > *Top Attacks* > *SPP* before the page fully loads may produce a corrupted file.
1135116	*Dashboard* > *System Resources* expanded timeline graphs may occasionally show Month/Day-of-Month (Jul 27) instead of Day/Day-of-Month (Sun 27).

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.

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.

www.fortinet.com