Release Notes

FortiDDoS-F 7.2.2

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

November 28, 2025
FortiDDoS-F 7.2.2 Release Notes

TABLE OF CONTENTS

Change Log

Date	Change Description
November 28, 2025	FortiDDoS-F 7.2.2 Release Notes initial release

Introduction

This Release Notes covers the new features, enhancements, resolved issues and known issues of FortiDDoS version 7.2.2 build 0836.

Special Notes

Upgrade any FortiDDoS F-Series firmware Release directly to 7.2.2. No intermediate steps are required.

Special note for when upgrading to 7.2.2

- If you are using DNS LQ Populate, before upgrade, go to *Global Protection* > *DNS LQ Populate* > *Valid FQDN* table and Search for the astersik character "*". If this returns FQDNs, after upgrade, go to *Global Protection* > *DNS LQ Populate* and disable *FQDN Check* which is enabled by default in 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.

Manual traffic bypass may not be enabled 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 7.2.2 offers the following new features and enhancements:

- Three additional tables are added to *TOP ATTACKS* > *Summary*, for all SPPs:
  - *Attacked Destinations Drop Distribution by L3/4/7*, showing the % distribution of all attacks across each OSI Layer, for the *Top 20 Protected IPs*.
  - *Attacked Destinations Drop Distribution by Category*, showing distribution % by top 20 ACL, Anomalies, Floods, and Validations, for the *Top 20 Protected IPs*.
  - *Attacked Destinations Drop Distribution by Attack Event*, showing distribution by Attack Events, for the *Top 20 Protected IPs*.

  Some graph pages have been re-arranged for easier use:
  - *Monitor* > *TRAFFIC MONITOR* > *Layer 3/4/7* > *Layer 4* > *SYN*: The SYN-ACK graph is now directly below the SYN graph allowing easy comparison of SYNs in one direction with SYN-ACKs in the opposite direction.
  - *Monitor* > *TRAFFIC MONITOR* > *Layer 3/4/7* > *Layer 7* > *DNS*: The DNS Response Code graph is now directly below the DNS Query graph, allowing easy comparison of DNS Queries in one direction with DNS Responses in the opposite direction
- Context sensitive help is added for all GUI pages.
- New Scalar Thresholds and graphs are added for:
  - *Monitor* > *TRAFFIC MONITOR* > *Layer 3/4/7* > *Layer 3* > *Other* tab for UDP Fragments per Destination. This Threshold reduces the impact of DNS Reflected Response and other floods that frequently include UDP Fragments. Useful for SPPs with multiple firewalls, and other outbound users of DNS.
  - *Monitor* > *TRAFFIC MONITOR* > *Layer 3/4/7* > *Layer 4* > *Ports* tab: UDP Destination Port 53 per Destination. This Thresholds reduces the impact of non-DNS UDP attacks to Port 53 to a single destination rather than the entire SPP. Useful for SPPs with multiple DNS servers or other devices that have UDP Port 53 open (and firewalls protecting them).
  - *Monitor* > *TRAFFIC MONITOR* > *Layer 3/4/7* > *Layer 7* > *DNS* > *DNS Rcode 0 per Destination*. This threshold reduces the impact DNS Reflection Floods that have found a way to use "good" responses in the flood. Useful for SPPs with multiple firewalls, and other outbound users of DNS.
  - Email security has been improved with the addition of a custom **FQDN** field in *System* > *Admin* > *Settings*.
  - For 2000F/3000F models, where optical transceiver ports are cross-connected to the optical bypass module, manually setting which port-pairs are connected to the bypass modules shows bypass status for those port-pairs (links) on the *Network* > *Interface* page.
  - An FQDN Check option (enabled by default) has been added to the DNS LQ Populate feature to prevent FQDNs with illegal special characters from being added to the table. Although these characters are invalid, Bind9 permits “*” within FQDNs beyond its typical wildcard use. If you use DNS LQ Populate, please refer to the 7.2.2 Release Notes for details.
  - IPv6 geolocation database management has been improved to provide more accurate and reliable location data.
  - IPSec Tunnel Endpoints now monitor only Protocol 50 (ESP/IPsec), excluding IPsec NAT Traversal over UDP 4500 and IKE over UDP 500. This enables limiting ESP traffic to specific remote IPs without disrupting home or roaming users who rely on NAT Traversal, while IKE anomalies and thresholds continue to protect against IKE floods.

- The *Dashboard* > *TOP ATTACKS* > *SPP* tables can be added/removed from the page using *Widget Control* options.
- TCP Port Low Traffic Threshold maximum setting range is increased from 0-65535pps to 0-262,140pps for high traffic environments
- Event Log filtering speed is improved for higher efficiency.
- GUI labels have been improved for Chinese (simplified), Japanese, Korean, and Spanish.
- Added *Bypass Reversed Traffic* option in *Global Protection* > *Deployment* for use in networks where traffic may be hair-pinned back through FortiDDoS. Traffic is ignored but is still processed and will affect system throughput.
- TCP Profile Foreign Packet Threshold, if used with Foreign Packet Validation (FPV), is now persistent if FPV is disabled and then re-enabled. There is no requirement to record or remember the threshold when testing.
- An new graph for *Non-IP Ethertypes* is added to *Monitor* > *TRAFFIC MONITOR* > *Interface*. This graph is intended to show other types of traffic that are passed through FortiDDoS transparently but can affect overall throughput of the system.
- DNS Suspicious Sources has been updated to highlight sources that generate large volumes of NxDomain or NoData responses. This parameter still requires symmetric traffic and is not included in automatic System Recommended Thresholds; it must be configured manually if needed. Use caution, as floods can be relayed through public anycast or mobile provider recursive DNS servers, where randomized subdomains bypass rate limiting and caching. Blocking these servers' unicast IPs is not recommended; DNS LQ Populate remains the most effective mitigation.
- Additional tables are added to the customer and full debug files for improved offline analysis.
- New geo package no longer supports region; All existing configurations with "<county, region>" will be converted to "Other county".

Hardware and VM support

FortiDDoS 7.2.2 supports the following hardware models:

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

FortiDDoS 7.2.2 is NOT compatible with any FortiDDoS A- / B- / E-Series hardware.

FortiDDoS Release 7.2.2 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 7.2.2 release. For inquiries about particular bugs, please contact Fortinet Customer Service & Support.

Bug ID	Description
1117903	External logging files are modified to improve GUI performance under very heavy flooding. This issue has not been seen in the field.
1179746	In *Dashboard* > *Top Attacks* > *SPP*, if a PDF download is requested before the page has fully loaded, the file could be corrupted or missing components.
1192205	If *Adjust filter for all tables* was disabled, the filter options did not appear in the individual tables unless the header bars are clicked. The fix adds filters to header bar in each table immediately. Note, using different filters for different tables can be very confusing and is not recommended.
1194133	The *Monitor* > *TRAFFIC MONITOR* > *Interface* > *VLAN graph* Y-axis displayed *Drop* instead of *Throughput*.
1194677	During downgrade via Boot Alternate Firmware, SPP Traffic Statistics were not deleted.
1195054	The vertical scroll bar was missing from the *TRAFFIC MONITOR* > *SPP* page.
1198955	IPv6 addresses may not be correctly displayed in per-Source flood logs.
1199040	The Source IP address shown in DNSSEC UDP Asymmetric Response Source Flood logs may have reversed octets.
1203554	The *IP Profile* > *IP Fragment Check* (Fragment ACL) did not block IPv6 fragments.
1203702	Packets dropped due to DNS UDP Query (FQDN Allow List unmatched) did not appear in all relevant *Drops Monitor* > *Layer 7* > *ACL graphs*.
1207436	When editing existing DDoS Attack SNMP Trap Receiver information (for example to change the receiver IP address) the hidden password field (****) was updated with those characters, with unexpected results.
1208672	If a PDF report was requested from *Dashboard* > *Top Attack* > *SPP* when the page had not fully loaded, tables were missing. PDF icon is now disabled until the page is fully loaded.
1211584	Packets dropped due to Blocklisted Domains were reported as "DNS Blocklisted Domains (Domain Reputation)". This has been corrected to "DNS Blocklisted Domains".
1212866	A *Global Protection* > *Proxy IP* hash issue could result in a dataplane restart. Please note, the Proxy IP feature is ineffective in modern networks and should no longer be used.

Bug ID	Description
1222116	Attack log detail for IPv6 SPP ACLs sometimes showed the wrong Subnet (IPv4)
1222499	ACL Attack Log details table sometimes did not display the ACL name.

Common Vulnerabilities and Exposures

Release 7.2.2 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 7.2.2 release. For inquiries about particular bugs, please contact Fortinet Customer Service & Support.

Bug ID	Description
1223969	*System Resource* graphs may show Month/Day-of-month instead of Day-of-month/Month for some periods selected.
1220784	CSV download of filtered event logs downloads all event logs without filtering
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.
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.

Bug ID	Description
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.
1212811	DNS UDP Unsolicited Response (DQRM, which is only used with symmetric traffic) reports the Protected (ephemeral) port. For clarity and consistency, it should report Source Port 53.

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.

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