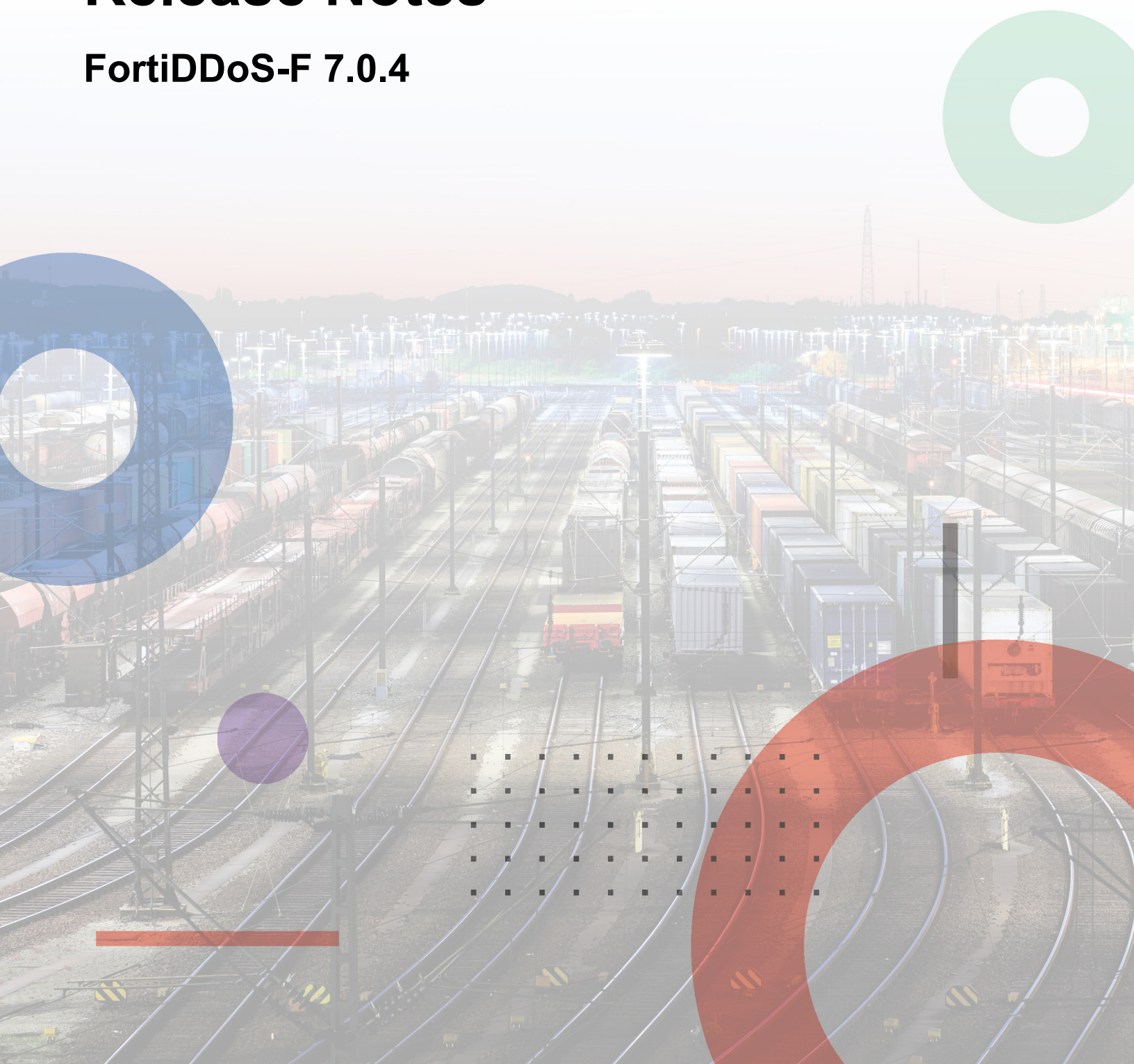
Release Notes

FortiDDoS-F 7.0.4



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

February 7, 2025
FortiDDoS-F 7.0.4 Release Notes

TABLE OF CONTENTS

Change Log

Date	Change Description
February 7, 2025	FortiDDoS-F 7.0.4 Release Notes initial release

Introduction

This Release Notes covers the new features, enhancements, resolved issues and known issues of FortiDDoS version 7.0.4 build 0746.

Special Notes

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 as a security improvement. The option can be re-enabled by the user if desired.

  After upgrade, always open the GUI via a private browser window or refresh the browser cache.
- On upgrade to 7.0.1, 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 will 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.

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-F7.0.4 offers the following new features and enhancements:

- In HA deployments, users can create Traffic Statistics on the Primary system and automatically merge them with Traffic Statistics from the Secondary system when they are created there. This should be done before setting Thresholds on the Primary, which then synchronizes the merged Thresholds to the Secondary.
- FDD-3000F can automatically create Layer 3 and Layer 4 Distress ACLs (ADACLs) under large floods
- For improved readability on smaller screens, *Dashboard* > *Top Attacks* automatically switches from a two-column to a single-column format. Additionally, all tables can be expanded to full-screen view.
- Optionally, low traffic rates on links can be detected, signaling the HA partner to pause Foreign Packet validation. This assumes that loss of traffic indicates diversion to the partner, rather than a link failure.
- Added a separate Attack Log event for SYN with Payload feature in TCP Profile.
- The *Dashboard Status* now displays the last 20 Emergency, Alert, or Critical event logs, with colored badges indicating the count for each type.
- FortiDDoS adds IKE (IPSEC setup over UDP 500) anomaly and flood protection.
- Attack Logs can now be filtered by drop count, allowing users to specify a threshold manually or select from the Drop Count column. The column also supports sorting in ascending or descending order.
- Enhanced link status signaling for improved communication with the HA partner.
- FDD-300F updates:
  - Distress ACLs do not sync from the HA Primary to the Secondary.
  - System-generated Automatic Distress ACLs (ADACLs) operate independently and are created on either HA partner as needed.
- FortiDDoS SPPs monitor and set Thresholds for the top 512 FQDN rates in DNS Responses. This is an additional DNS Response flood mitigation along with DQRM or Rcode Thresholds.
- FortiDDoS now shows outbound system-generated validation packets for SYN, HTTP and DNS mitigation operations.
- Added CLI commands to check SSD integrity (S.M.A.R.T). The "checklogdisk" CLI command has been removed as it was ineffective and disruptive.
- The system can be set to ignore VLAN traffic that passed through FortiDDoS, since it is normally Private IP to Private IP and would normally display in the default SPP.
- FortiDDoS now supports entering a list of VPN local and remote IPs for IPSEC (Protocol 50/ESP/IPSEC), IKE (UDP 500), and IPSEC NAT Traversal (UDP 4500). Only VPN traffic will be allowed between these IP pairs. All other traffic will be rejected.
- The *Dashboard* > *Top Attacks Summary* page now includes SPP links, allowing direct navigation to the corresponding SPP on the Top Attacks SPP page.
- *Attack Log Backup* has been removed since the attacks logs can be downloaded from the Logs page or via the Debug files.
- TTL options are removed from FDD-3000F Distress ACL settings since TTL is not supported.
- Cloud signaling devices now have support only for third-party service providers.
- New *Last Successful Attack Sent* column is added in the *Signaling Devices* table, which shows the timestamps of last successful attack sent for a particular signaling device.

Hardware and VM support

FortiDDoS 7.0.4 supports the following hardware models:

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

FortiDDoS 7.0.4 is NOT compatible with any FortiDDoS A- / B- / E-Series hardware.

FortiDDoS Release 7.0.4 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 7.0.4 release. For inquiries about particular bugs, please contact Fortinet Customer Service & Support.

Bug ID	Description
1075184	*Top Attacks* page table columns for *Drops and Events* sometimes did not sort correctly when using the header sort links.
1080194	Diagnostic information for 7.0.3 VMware/KVM VM04 and VM08 displayed the incorrect number of SPPs
1087992	There was no validation to prevent duplicate IPs in the *Global Protection* > *GRE Tunnel Endpoint* list. While this posed no major issue, it could reduce the total number of IPs allowed in the list.
1089446	If DNS LQ Populate is enabled, malformed FQDNs in Queries can cause the LQ process to crash and restart the VPP, leading to logdisk fill. This issue with DNS LQ Populate and logdisk fill has been resolved.
1091743	Report and alert emails may be tagged as SPAM due to missing message-ids.
1093684	If Attack Log SNMP traps were set for v3 with Authentication and Privacy and then changed to v2, the Auth and Privacy fields still showed (but obscured).
1093715	SPP names were displayed incorrectly on the Attack Log Remote settings page.
1094259	Attack logs were not generated for DNS TCP Query flood drops. This issue has been corrected.
1099065	DNS Profile FQDNs and Regex were limited to 255 characters, but longer strings were truncated without warning. Now, entries exceeding 255 characters are rejected.
1111080	The Change Password button in *System* > *Admin* > *Administrator* did not update the password; the workaround was to use the *Edit* button instead.
1111506	Searching the Protection Subnets List for an IP address within a large subnet could fail.
1092640 1092698	If formatlogdisk was performed, the SNMP trap process could sometimes fail to locate the correct file and crash.
1098949 1099063	The HA Secondary could enter bypass mode after joining HA and reloading the configuration.
1078344	Some diagnostic commands could incorrectly report the number of SPPs for VM-04 and VM-08, though the configurable values remain correct at 4 and 8.

Common Vulnerabilities and Exposures

Release 7.0.4 contains precautionary upgrades to various common source modules.

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

Known issues

This section lists the known issues in FortiDDoS-F 7.0.4 release. For inquiries about particular bugs, please contact Fortinet Customer Service & Support.

Bug ID	Description
0693789	When FortiDDoS-VM is operating on a virtual machine with underlying hardware supporting SR-IOV, disabling ports leads to unexpected results.
0678445	Purging a large number of ACLs from an SPP can take more than 30 seconds with no progress indication.
0882029	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.
0904954	After saving SPP or Global ACL Lists, re-ordering will only work for 1 step up or down from current location in the list.
0918768 0923612 0924121	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.
942816	FortiDDoS VM manual force FortiGuard update will not work. There is a workaround via shell which will be documented.
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.
1002526	FortiDDoS 2000F 40G QSFP+ Transceivers are not working correctly. This problem is fixed but requires an RMA for any systems shipped prior to 2024-05. Please contact FortiCare for confirmation.
1011488	DNS Known Opcode Anomalies are shown as DNS Header Anomaly drops. This is design Intent and won't be changed. It is documented in the 7.0.1 Handbook.
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.
1016007	Large DNS Zone Transfer responses are dropped due to the DNS Exploit Anomaly: TCP buffer underflow. DNS Zone Transfer inbound Responses are typically rare on FortiDDoS-protected DNS servers, except for backup servers. Master servers may experience outbound Zone Transfers that could result in drops, but these will not occur in Detection Mode. To maintain security, review all outbound drops in Detection Mode and disable any anomalies in the relevant DNS feature profiles. DNS and other anomalies are not DDoS vectors; they are "clean-pipe" features that can be disabled if needed.

Bug ID	Description
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.
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.
1105109	Bypass module state change inline-to-bypass or bypass-to-inline causes a brief outage (associated ports go down and up in less than 1 second). This "flap" is enough to trigger BGP changes for some customers. If this is disruptive, the only option is an external bypass bridge like the Niagara 3808.
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.
1118829	When changing SPPs for the *TRAFFIC MONITOR* > *SPP* > *System Generated Packets* you must refresh the graph (circular icon) to correctly display the graph.

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