FortiDDoS-F - Release Notes

Version 6.1.1

FORTINET DOCUMENT LIBRARY
https://docs.fortinet.com

FORTINET VIDEO GUIDE
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/support-and-training/training.html

NSE INSTITUTE
https://training.fortinet.com

FORTIGUARD CENTER
https://fortiguard.com/

END USER LICENSE AGREEMENT
https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK
Email: techdoc@fortinet.com

February 18, 2021
FortiDDoS-F 6.1.1 Release Notes
00-611-696305-20210218

TABLE OF CONTENTS

Change Log

Date	Change Description
2021-02-18	FortiDDoS-F 6.1.1 Release Notes initial release

Introduction

This Release Notes covers the new features, enhancements, and known issues of FortiDDoS version 6.1.1 build 0068.

FortiDDoS 6.1 features a clean-sheet new architecture that draws on more than 10 years of FortiDDoS' DDoS mitigation experience while providing a flexible and forward-looking solution to detect and mitigate Layer 3 to Layer 7 DDoS attacks for enterprise data centers. FortiDDoS uses machine learning and behavior based methods, and monitors hundreds of thousands of networking parameters to build an adaptive baseline of normal activity. It then monitors traffic against that baseline and defends against every DDoS attack.

For those familiar with FortiDDoS B- and E-Series, FortiDDoS 6.1 offers additional features, some changed functionality and some features that have been removed. A reference table is included for comparison.

What's new

FortiDDoS-F 6.1.1 offers the following new features:

- **HA Override** - High Availability Override (disable, use uptime or enable, use Priority) option has been removed but can be used as follows:
  - Normal HA Operation: Make Primary system a lower numeric Priority number and Secondary system with higher numeric Priority number.
  - HA by system uptime operation: Both system have same Priority number.
- **Mail fail logs** - FortiDDos will now generate event logs if the Alert Mail server is unreachable or authentication fails.
- **Service ports** - Both HTTP and HTTPS service ports can be configured per SPP.

FortiDDoS-F Series New features

FortiDDoS-F series is built on the feature base of FortiDDoS B/E-Series with these notable additions:

- VMware support with SR-IOV support where available
- NTP from E-Series on all models
- Additional SSL DDoS Mitigation settings
- 16x SPPs in1500F and 4/8/16x SPPs in VM04/VM08/VM16
- DNS Rcode Scalars are included in Traffic Statistics and System Recommendation
- NTP Scalars are included in Traffic Statistics and System Recommendations
- Split System Recommendation for Layer 4 Scalars/ICMP, TCP Ports and UDP Ports included from B/E 5.4.0
- Common UDP Source Reflection Ports are pre-populated in Global Service definitions for use with Global or SPP ACLs
- Service port definitions support Source Port or Destination Port. Source Port ACLs are very useful for permanently blocking kown UDP reflection ports.
- IP Address / Subnets definitions are created in the System menu and then assigned to Global or SPP ACLs, reducing multiple entries.
- Bogons IPs and/or Multicast IPs can be ACLed with option selection in any SPP.
- SPPs replace feature tabs with multiple Profiles for IP, ICMP, TCP, HTTP, SSL/TLS, NTP and DNS. One Profiles can be used by muliple SPPs or one SPP can use Multiple Profiles (TCP Detection and TCP Prevention, for example).
- Source MAC address for aggressive aging is configurable per SPP, if needed
- Strict Anomalies options are now included in several SPP Profile pages for Layer 2 to Layer 7 options.
- Cloud Signaling Thresholds are entered in both pps and Mbps (crossing either triggers Signaling. Thresholds are now per SPP Policy (subnet).
- SPP Policies (subnets) are entered for each Service Protection Policy (SPP) instead of globally.
- Explicit TCP thresholds are added for DNS Query, Question Count, Fragment, MX and ALL. B/E-Series has TCP Thresholds but they are hidden and the same as the UDP Thresholds.
- IP Reputation and Domain Reputation are included in IP and DNS Profiles and thus are optional per SPP.
- SSL/TLS Profile includes additional Cipher Anomaly option
- tcpdump-style packet capture
- Several formerly-global features such as IP Reputation are now set per SPP for better control
- Additional Known Method Anomalies available

Removed/Changed/Deferred Features

B/E-Series Functionality not included in this release:

- Support for FortiDDoS-CM Central Manager
- Security Fabric Integration with FortiOS Dashboard
- GTP-U support
- Distress ACL nor Auto-Distress ACL
- Multi-tenant support (SPP or SPP Policy Group)
- Fewer files included in Offline analysis file
- SPP Backup/Restore
- Attack Reports are Global only and are on-demand or on-schedule only. Report periods are Last 7 Days, Last Month or Last year only. (Removed per-SPP, per-SPP Policy, per-SPP Policy Group reports, on-Threshold reports and some time periods)
- REST API changes and requires documentation
- Log & Report > DDoS Attack Graphs
- SPP Policy Groups
- Log & Report > Diagnostics
- SPP-to-SPP Switching Policies
- Restrict DNS Queries to specific subnets
- System Recommendation Option for Actual or System Max Outbound Threshold (5.4.0)
- Traffic Statistics Option for Peak or 95th Percentile Traffic (5.4.0)
- Syslog RFC 5424 or Fortinet proprietary secure "OFTP" protocol (5.4.0)
- CLI Commands for IP Reptution nor Domain Reputation updates (5.4.0)
- Search for IP addresses within various ACLs (5.3.0)

VM limits

- VMs do not support Fail-Open option. Fail-Open support will be determined by the underlying server
- TCP Port Thresholds are calculated to 65,535 but Thresholds/Ranges are created for ports 1-1023 with one range for ports above 1023.
- TCP Port Graphs display traffic and drops for Ports 1-1023. Port 1024 displays peak traffic rate for any port from 1024-65,535 and total drops associated with any of those ports. Attack logs show full port range 1-65,535.
- UDP Port Thresholds are calculated to 65,535 but Thresholds/Ranges are created for 1-10,239 only with one range above that.
- UDP Port Graphs display traffic and drops for Ports 1-10,239. Port 10,240 displays peak traffic rate for any port from 10,240-65,535 and total drops associates with any of those ports. Attack logs show full port range 1-65,535 as well as reflected attack drops from ports 1-9,999.
- ICMP Type/Code Thresholds are calculated from 0-65,535 but Threshold/Ranges are created for 0-10,239 only. Indexes from 10,240 to 65,535 are included in one range.
- ICMP Type/Code graphs show indexes from 0/0 to 39/255 with all others showing in 40/0. Attack logs will show drops for Types/Codes for all Types/Codes from 0/0 to 255/255.

Hardware and VM support

FortiDDoS 6.1.1 supports the following hardware models:

- FortiDDoS 200F
- FortiDDoS 1500F

FortiDDoS 6.1.1 is NOT compatible with any FortiDDoS A- / B- / E-Series hardware.

FortiDDoS Release 6.1.1 supports deployment of FortiDDoS-VM04/VM08/VM16 in the following virtual machine environments:

- VMware

Known issues

This section lists the known issues in FortiDDoS-F 6.1.1 release. For inquiries about particular bugs, please contact Fortinet Customer Service & Support.

Bug ID	Description
626478	Trusted Hosts are not checked if LDAP/RADIUS/TACACS+ external authentication is used.
668077	RADIUS and other external authentication 2FA is not available in 6.1.1.
670473	The "TCP Session Idle Timeout" for IPv6 is fixed at 528 seconds.
672585	Very small, invalid DNS packets may be dropped even when no DNS Anomalies are enabled with no logging.
676495	The Monitor > Layer 3 > Other: Fragmented Packets graph does not show Thresholds for TCP/UDP/Other Fragments.
677407	After a large IP or Domain Blocklist has been successfully uploaded to FortiDDoS, there is no indication that it is present on the system (no count of entries and no ability to search for an entry). Download will download the list as a text file to confirm.
678433, 678434	Release 6.1.1 does not support LDAPS/STARTTLS
678445	Purging a large number of ACLs from an SPP can take more than 30 seconds with no progress indication.
679309	When configured with large numbers of ACLs and wide attacks across all ACLs, all logs may not show.
692550	Under heavy attack load, graphing may lag.
680412	The last x-axis label on the Dashboard Drops Graph is not always displayed.
685605	Under heavy flooding system may show DQRM memory drops when DQRM table is not full.
688477	Under very heavy, sustained flooding across a wide range of parameters, reporting may be delayed.
690017	For FDD-200F and FDD-1500F: After creating a Service Protection Profile, you may see event logs like this: SPP:sp3 RRD Mismatch, expected : 227 but got :110 These are harmless and can be ignored.
693817	Failed LDAP logins don't provide information on the failure.
693789	When FDD-VM is operating on a virtual machine and underlying hardware supporting supporting SR-IOV, it is unable to disable the data ports.

Resolved issues

The following issues have been resolved in the FortiDDoS-F 6.1.1 release. For inquiries about particular bugs, please contact Fortinet Customer Service & Support.

Bug ID	Description
607752, 608432	Test Connectivity function was not working for RADIUS and LDAP.
635405	The system may lose recent attack logs after reboot.
637792	Log backup cannot be imported
668205	DNS packets with same Source and Destination address:port are mishandled. The first packet is allowed, subsequent packets are dropped but without logs or graphs.
668229	IPv6 performance specifications are lower than IPv4
669294	DNS Cache expiries are about 2x the actual TTL of the FQDN.
680379	Heavy traffic in 16 SPPs could result in slow reporting.
680412	The Dashboard Drop graph did not perfectly match the Attack Log table time-period.
680482	Errors when creating/modifying Threshold did not result in an error message.
680484	Once a Threshold is created, only the data rate fields for that threshold may be modified. Other fields (like port numbers) appeared to be editable but were not. Non-editable fields are now grayed-out.
680826	The FortiView SPP detail Countries graph did not always show a full 1-hour period.
680961	Filtering Attack Logs lead to inconsistent log lists.
681148	Dashboard > Top Attacks PDF output period did not match the period of the table.
681159	Estimated (Adaptive) Thresholds were not calculating correctly.
681337	When configuring a Service ACL with a Source Port, the Destination range start Port could not be configured.
683957	Overlapping ACL addresses were not allowed even though different types. For example 0.0.0.0/0 allows all but then Geolocation could not deny a country.
685548	Login Username was not displayed on GUI (always "Admin")
686946	ICMP and URL ACLs were not blocking traffic.
689504	Dropped packets based on a URL ACL were still shown as egress packets (not dropped on the graph).
689982	For VMS: After creating a Service Protection Profile, you may see event logs like this: SPP:sp3 RRD Mismatch, expected : 227 but got :110
690117	Some valid ICMP Types/Codes were included in the ICMP Type/Code Anomaly option.
690641	Sometimes when filtering for date and other options, the date selector was not

Bug ID	Description
	removed from the GUI.
690942	[FortiView] Attack TCP and UDP Drops were showing bits instead of packets.
690985	Default Low Thresholds and Percentage Multipliers in System Recommendations were not saved/persistent after setting Thresholds.
691069, 691074, 691077	Some tables did not show an updating spinner when user selected Refresh.
691823	Overlapping IP Address, IP range and/or IP/Netmask ACLs with Geolocation ACLs may have been rejected.
692277	The monitor graph for DNS anomaly UDP zone transfer was missing.

Upgrade notes

On the VM platform, to avoid the VMware network broadcast storm for the new deployment, each WAN/LAN interface pair is disabled by default so that traffic will not pass through.

In the initial deployment, please remember to enable the WAN/LAN interface pair via CLI

```
# config system l2-interface-pair
# edit l2-port1-port2
# set status enable
# next
# end
```