FortiDDoS-F - Release Notes

Version 6.2.0

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://www.fortiguard.com

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

FEEDBACK
Email: techdoc@fortinet.com

August 5, 2021
FortiDDoS-F 6.2.0 Release Notes
00-620-730305-20210805

TABLE OF CONTENTS

Change Log

Date	Change Description
2021-08-05	FortiDDoS-F 6.2.0 Release Notes initial release

Introduction

This Release Notes covers the new features, enhancements, resolved issues and known issues of FortiDDoS version 6.2.0 build 0211.

FortiDDoS F-series 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 S-Series, FortiDDoS F-series 6.2.0 offers additional features, some changed functionality and some features that have been removed. A reference table is included for comparison.

What's new

New features

- SYN/ACK Scalar Thresholds for asymmetric traffic. With asymmetric traffic, FortiDDoS normally needs to assume an inbound SYN/ACK represents the response from an unseen outbound SYN and creates a connection table entry. This leaves the system/user open to advanced SYN/ACK floods. In 6.2.0 the following Thresholds are visible only when the system is in Asymmetric Mode with Asymmetric Mode Allow Inbound Synack enabled:
  - SYN/ACK - aggregate rate of all SYN-ACKs into the SPP Protected Subnets
  - SYN/ACK per Destination - maximum rate of SYN-ACKs to any single destination in the SPP Protected Subnets

  Note:
  - SYN/ACK Thresholds are not automatically learned and System Recommendations are not created. Use the above graphs to calculate peak rates and create manual thresholds.
  - There is no Adaptive Threshold for these Scalars.
  - These thresholds function on INBOUND traffic only.
- DTLS Profile is added to Service Protection Policies. Use DTLS to prevent DTLS direct and reflection attacks on all services, unless operating in Asymmetric Mode.
- Possible UDP Reflection Flood is added from B/E-Series with similar functionality. Any drops associated with UDP Port Thresholds FROM Ports 1-9999 are shown in the attack logs as Possible UDP Reflection Floods. This protects from and identifies any of the more than 30 currently known UDP reflection ports like 19, 111, 389, etc. as well as identifying future reflections on any port lower than 10,000. FortiDDoS F-Series does no support UDP Service ports in 6.2.0.
- System Recommendation now has an option to use actual outbound traffic statistics for outbound thresholds or set all outbound thresholds to system maximum (default and recommended).
- Treatment of Global ACLs changes with a dedicated "SPP" for all kinds of Global ACLs. New items added for:
  - *Dashboard > Top Attacks > Global: Global ACL Attack table*
  - *Monitor > Drops Monitor >Global: Graphs of Global Aggregate and ACL Rule Drops*

  Note: Global ACLs always drop identified packets and do not follow Detection/Prevention settings per SPP.
- A Protection Subnets List GUI page is added to list all Protection Subnets for all SPPs and the Detection Mode/Prevention Mode status of the SPP hosting the Protection Subnet. Protection Subnets cannot be edited from this page
- Blocklisted IPv4 and Blocklisted Domains UI's have been improved to include showing the number of addresses/Domains applied, last update date, add and delete individual addresses/Domains and search for an address/Domain in the lists.
- Navigation is available between Service Protection Policies when in the SPP editing pages.
- FortiGuard scheduled updates are changed to Daily or Weekly only. More frequent updates were not providing additional information.
- Reboot and Shutdown commands are added to the top-right user logout menu.
- The Domain Reputation attack log event has been separated from the Domain Blocklist event.
- FortiView Threatmap improves time-period selection for display
- Additional tool-tip date and time information is available on longer-period graphs (week/month/year).
- Added CLI command to restart nginx (GUI)
- Added CLI command get bypass-status to show inline/bypass status of associated ports.
- Added CLI command diagnose dataplane geo-ip <IPv4 address(no mask)>. This allows user to check within which geolocation a specific IPv4 address is located.

- Labeling, graph units, borders, field sizes, event log, attack log and tool tip information and other improvements added throughout the GUI.
- CSV downloads for various tables such as Attack Logs are not 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)
- CSV downloads for various tables such as Attack Logs are not available.

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 6.2.0 supports the following hardware models:

- FortiDDoS 200F
- FortiDDoS 1500F

FortiDDoS 6.2.0 is NOT compatible with any FortiDDoS A- / B- / E-Series hardware.

FortiDDoS Release 6.2.0 supports deployment of FortiDDoS-VM in the following virtual machine environments:

- VMware
- KVM

Resolved issues

The following issues have been resolved in the FortiDDoS-F 6.2.0 release.

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

Bug ID	Description
692418	FortiDDOS 6.2.0 is no longer vulnerable to the following CVE-Reference: CVE-2020-15935
661551	In HA systems the Authentication Default Access Strategy for any remote authentication (LDAP, RADIUS, TACACS+) was not synchronized with the secondary system.
665604	When setting up a new user via CLI, if remote authentication was selected, the password option should not be available.
667108	After creating a new admin user with remote authentication, that user could be edited to become a local user but since this user has no local password there was no access. Delete remote authentication users to add them (with password) as local users.
608437 608438 608439	Default Access Strategy for remote authentication (RADIUS, LDAP, TACACS+) shows options that are not valid for F-Series products. Result can be failure to accept configuration.
633151 634481 637835	Some combinations of UDP and TCP DNS Queries had unexpected results.
635454	During SPP reset, chagnes were allowed on the SPP. SPP will be locked until rest is complete.
636796	If DNS Response packets are sent to another FortiDDoS monitoried "service" port such as 123, or 443 will be treated NTP or DTLS and will not be inspected by DQRM. This is not likely to result in missed mitigations if NTP and DTLS Anomalies are set but the Attack logs will reflect the "service" on the destination port and not DNS..
670602	Horizontal scroll bars did not appear for various window sizes on some OS and Broswer combinations
676265	Primary HA system authentication changes appeared to not synchronize on secondary HA system - GUI issue.
676495	The Monitor > Layer 3 > Other: Fragmented Packets graph does not show Thresholds for TCP/UDP/Other Fragments.
680358	When uploading a firmware image file for upgrade the GUI was slow to show that the upload was proceeding.

Bug ID	Description
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
690937	On early VM releases, when creating a number of SPPs, some might not have complete databases.
692550	Under heavy attack load across a large number of ports, graphing may lag.
693196	While thresholds work, attack Log and drops graph info for Excessive Concurrent Connections Per Source and Excessive Concurrent Connections Per Source flood is missing
693817	Failed LDAP logins don't provide information on the failure.
695337	Under stress load REST API crashlogs were generated.
695928	When a Service Protection Policy is created, significant background work is required to set up the database which takes some time. During this time some changes related to the SPP could be requested by the user that affected the SPP. All changes to the SPP are now locked until the SPP is fully setup.
695929	When updating firmware, the system might generate spurious crashlogs which were harmless.
696018	Depending on authentication protocol, system might not failover correctly to secondary RADIUS server.
700106	FortiGuard IP Reputation or Domain Reputation updates did not create event log.
700345	Invalid ICMPv6 Type Code drops were shown as ICMPv4.
700366	SYN Flood events were defined as "periodic" instead of "event" which could slow reporting in logs and graphs.
701146	If Traffic Stats generation was in process and user requested System Recommendation, depending on use of GUI and/or CLI for each command, System Recommendation started with unexpected results.
701233	MIB file attack event labels did not match attack log labels.
702780	DNS Block Identified Sources does not work under DNS fragment and DNS Unsolicited Responses
706508	Some drop graph X-Axis labels were offset so that the drop graph did not match the attack log time-stamp.
709425	HA Secondary physical port attributes were synched with Primary.
712109	In HA pairs, time change was not allowed on Secondary.
712472	Disabling and re-enabling port pair 1-2 might prevent the pair from processing traffic.

Bug ID	Description
718592	DNS Pointer loop anomalies were not detected on some types of DNS packets.
720062	DNS UDP Question Count Threshold was not working. Qcount Floods did not trigger validations.
720062	DNS UDP Question Count Threshold was not working. Qcount Floods did not trigger validations.
720068	DNS UDP All/Any and MX count Thresholds were not working. Threshold violations did not result in validations.
721536	Most Active Destination graph and FortiView tables didnot display. Most Active Destination by default is not enabled and is normally only set manually by ISPs.
725152	If TCP Profile > Aggressive Aging Feature Control > Slow TCP Connections was disabled, then TCP Slow Connection Protection did not work, no matter the settings.
725253	TCP Profile > TCP Session Settings > TCP Session Extended Source Type IPv6 continued to use TCP Session Idle Timeout instead of TCP Session Extended Timeout.
725255	TCP Profile would allow use of a Geolocation service (country) for TCP Session Extended Source Address IPv4 but this did not work. TCP Session Extended Source Address IPv4 is intended for use with individual addresses or addres groups only.
725257	Source IPs (IPv4/IPv6) assigned to TCP Session Extended Source timeout should also override any Slow Connection settings for that TCP Profile but Slow Connection settings applied to them.
725872	Traffic inside GRE tunnels was not monitored correctly.
726193	Upgrading VMs from 6.x.x (< 6.1.4)to 6.2.0 will result in lost configuration. Upgrade from 6.x.x to 6.1.4 and then to 6.2.0.
726277 726528	Slow Connection drops may not have appeared in Dashboard > Drops widget.
726580	Fragmented SYN, FIN, RST packets may not have been tracked correctly.
726808	DNS TTL Too Long Anomaly was miss-configured. Correct configuration: TTL Too Long Anomaly enabled: TTL < or = 7 days allowed. Longer dropped. TTL Too Long Anomaly disabled: TTL < or = 30 days allowed. Longer dropped.
726808	DNS TTL Too Long Anomaly was miss-configured. Correct configuration: TTL Too Long Anomaly enabled: TTL < or = 7 days allowed. Longer dropped. TTL Too Long Anomaly disabled: TTL < or = 30 days allowed. Longer dropped.
726850	Alertmail Test Connectivity may send a blank password resulting in a test failure.
727174	SNMP MIB get for Memory Usage is incorrect.
727177	If Mgmt1 port was configured with Allow Ping disabled, it could not ping outbound. Outbound ping must be allowed even if inbound pings are ignored.

Bug ID	Description
727974	"Top Successful Logins" and "Top Failed Logins" may not have been reported in user-generated Reports
727976	Emailed HTML Reports had incorrect reference links and would not display in a browser. Emailed PDF or Word Reports worked.
728633	Full global subnets for IPv4 (0.0.0.0/0) and IPv6 (::/0) should only be allowed in the default SPP. They could be assigned to other SPPs prior to 6.2.0.
728807	After formatlog disk, GUI login may not appear. Reboot restores the GUI as a workaround.
728833	KVM VMs did not allow configuration of the number of SPPs stated in the datasheet.
730255	Editing previously-created DNS Resource Records did not work.
730255	Editing previously-created DNS Resource Records did not work.
730292	FortiGuard update event logs show under "config" instead of "update"
730372 730373	New TCP Profiles created from the GUI automatically set the Extended Timeout Policy for all users and this could not be changed from the GUI.
730996	If user changed system time, all data collection might stop. Note, if system time must be changed after a period of use the BEST outcomes are the following: - If system time is changed backwards, no new graphing is seen until the new system time is after the previous system time, since data is already in the dayabases for that period. If you set the time back one hour, no new graph data will show for an hour. - If system time is change ahead, graphs will show a gap in time with no data. Recommendations: - Adjust the time-zone to create the correct offset in hours (assuming change is in hours). Adjusting time zone has no impact on graphs. - After time change, use CLI to formatlogdisk and clear all traffic and drop data - ALWAYS USE NTP to ensure accurate time. System clock accuracy is poor and drifts steadily. It is important to have accurate NTP-based timestamps to correlate events.
731324 731328 731364	Drops shown in FortiView and Top Attacks may be different.
731389	On FDD-200F using ports 15 and 15 can result in a system crash.

Known issues

This section lists the known issues in FortiDDoS-F 6.2.0 release. For inquiries about particular bugs, please contact Fortinet Customer Service & Support.

Bug ID	Description
678433	Releases 6.1.x and 6.2.0 do not support LDAPS/STARTTLS
678434	TACACS+ Secondary server is not supported.
731320	During SPP creation, it takes several seconds for the back-end databases to be configured for each SPP. If the system is interrupted by a reboot, formatlogdisk or power failure, the databases may not be completed. The symptom will be missing graphs in some or all SPPs. After upgrading, adding an SPP, or after traffic is passing through FortiDDoS, user should: 1) Check that Dashboard > SPPs graph widget is showing traffic.If so, all databases are present.If not showing traffic (and traffic is present): 2) Check Monitor > SPPs. Cycle through all SPPs looking for traffic on each one.If any are not showing traffic use CLI execute spp-rrd-reset spp <rule_name> to reset those databases. 3) If in doubt, use CLI execute rrd-reset All (note: "All"). This should have no affect on existing traffic or drop data nor logs.It is purely a graphing issue.
714534	If setting Private Key and Certfiicate from CLI, the event log creates a blank message.Use GUI.
695645	Under rare conditions, generating multiple Certificates after a configuration restore can stop the GUI.
693789	When FDD-VM is operating on a virtual machine and underlying hardware supporting supporting SR-IOV, disabling ports leads to unexpected results.
686846	Online SCEP Enrollment Method of Certificate generation fails.
678445	Purging a large number of ACLs from an SPP can take more than 30 seconds with no progress indication.
676634	GUI will allow multiple and overlapping Hash entries various HTTP Thresholds like URL, Host, etc. Use care when manually entering indexes.
672585	Very small, invalid DNS packets may be dropped even when no DNS Anomalies are enabled with no logging.
671973	Global Service ACL explicitly for SCTP may have shown on earlier releases. This has not been implemented. Use Protocol # 132.
668077	External Authentication (RADIUS, LDAP, TACACS+) does not support 2-factor authentication.
638555	If multiple Questions are sent in the same TCP Query session, and QD Count not equal to 1 is not enabled, system ignores TCP Query Threshold. Use QDCount

Bug ID	Description
	not equal to 1 anomaly, since no DNS server will respond to 2 simultaneous Questions in one Query.
637835	Multiple Queries in a single TCP DNS session are allowed to exceed TCP DNS Thresholds. Fortinet experience is that this is a very rare possibility.To work around, setting QDCount not One in Query will drop these Queries as anomalies.
634691	FortiDDoS VM does not support a console port.
630479	If multiple changes are made on a GUI page before saving, an event log is created for only 1 change.
626478	Release 6.1.x and 6.2.0 do not support Trusted Hosts for LDAP / RADIUS / TACACS+.
626478	Trusted Hosts are not checked if LDAP/RADIUS/TACACS+ external authentication is used.
670473	TCP Session Idle Timeout for IPv6 connections is 528s no matter what is set in the timeout field.
677407	Upload of bulk IP address lists for Blocklist is supported, as well as download of that list. Deletion of IP addresses, and searching for IP addresses is not supported in 6.1.0

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
```