FortiDDoS Release Notes

VERSION 5.0.0

FORTINET DOCUMENT LIBRARY

http://docs.fortinet.com

FORTINET VIDEO GUIDE

http://video.fortinet.com

FORTINET BLOG

https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT

https://support.fortinet.com

http://cookbook.fortinet.com/how-to-work-with-fortinet-support/

FORTIGATE COOKBOOK

http://cookbook.fortinet.com

FORTINET TRAINING SERVICES

http://www.fortinet.com/training

FORTIGUARD CENTER

http://www.fortiguard.com

END USER LICENSE AGREEMENT

http://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK

Email: techdocs@fortinet.com

12/28/2018

FortiDDoS 5.0.0 Release Notes

Revision 1

TABLE OF CONTENTS

Change Log **4**
Introduction **5**
What's new **6**
Hardware support **7**
Image checksums **8**
Firmware Installation and/or Upgrading **9**
Downgrading **10**
Factory reset **11**
Resolved issues **12**
Known issues **13**

Change Log

Date	Change Description
12/28/2018	Initial version of FortiDDoS 5.0.0 Release notes.

Introduction

This document provides a list of new features and known issues for FortiDDoS 5.0.0 build 0004, including TP2ASIC Version: 500001f7 Date: Dec 20, 2018.

FortiDDoS Release 5.0.0 is available for FortiDDoS E-Series appliances ONLY and is the first release available for this platform.

FortiDDoS is a network behavior anomaly (NBA) prevention system that detects and blocks network attacks that are characterized by excessive use of network resources. These attacks are known as Distributed Denial of Service (DDoS) attacks.

For additional documentation, please visit: http://docs.fortinet.com/fortiddos

What's new

FortiDDoS 5.0.0 release includes the following new features:

- Equivalent to B-Series Release 4.7.0 firware.
- Support for FortiDDoS E-Series appliances (FDD-1500E and FDD-2000E) which supports higher throughput and 10GE, 40GE and 100GE interfaces as well as 10/40/100GE Optical Bypass.
- The following features are new in FortiDDoS B-Series Release 4.7.0 and shown here for clarity:

    - Effective Release 4.7.0, FortiDDoS is integrated into Fortinet Security Fabric. FortiGate and other Security Fabric products will be able to poll tabular and graphical data to create high-level single-pane-of-glass views of interconnected appliances in the Fabric. All configuration of the Security Fabric displays will be done from the higher-level appliance or management package. The only information required are administrative login credentials for the appliance you wish to appear on the Security Fabric GUI. There are no setting requirements for FortiDDoS. Note that FortiOS and other Fortinet products may not support FortiDDoS until later releases of firmware.
    - FortiDDoS now supports LDAPS and Bind types.
      For more information, see Configuring LDAP authentication.
    - FortiDDoS GUI now offers a search box on the left panel to find any menu items, settings and applicable keywords.
    - FortiDDoS can now export the SPP Policy list as a CSV spreadsheet to allow offline analysis and easier searching for specific subnet information.
      For more information, see Configuring an SPP policy.
    - All Outbound Scalar Thresholds are set to system Maximum to prevent virtual outbound drops than can result in real inbound drops. Thresholds can be modified by the customer.
    - Traffic Statistics algorithm has been modified to account for more 'spiky' traffic. This will be largely transparent to users.
    - More descriptive information is added in syslog messages.
      For more information, see Configuring remote log server settings for DDoS attack log.
    - Offline Analysis download button is available under **System** > **Maintenance**. This creates a zip file with the following files:
        - System configuration
        - CSV Traffic Statistics for every SPP and every Period used
        - CSV List of SPP Policies / Subnets
        - CSV of up to 20k Attack Log entries.

      These files can be used for offline analysis of attacks and system settings.
      For more information, see Backing up and restoring the configuration.

NOTE: **FortiDDoS E-Series 5.0.0 is NOT SUPPORTED by FortiDDoS-CM.**

Hardware support

This release supports the following hardware models:

- FortiDDoS 1500E
- FortiDDoS 2000E

NOTE: FortiDDoS A series and B series models are not supported.

Image checksums

Checksums are not required for this Release since it is pre-installed on the appliance.

Firmware Installation and/or Upgrading

This is the initial firmware release for E-series appliances and as such will come pre-installed on the appliance. There are no installation and/or upgrade procedures required.

Downgrading

Downgrading from this release is not possible. **Do NOT attempt a downgrade.** Contact Fortinet Support.

Factory reset

If you want to restore a system to factory defaults with no customer configuration or traffic data, do the following from CLI:

- `# execute formatlogdisk` - removes all traffic data.
- `# execute factoryreset` - removes all configurations.

Resolved issues

Since this is the initial release of FortiDDoS 5.0.0, there are no resolved issues.

Known issues

This section lists the known issues in FortiDDoS 5.0.0 release. For inquires about a particular bug, please contact Fortinet Customer Service & Support.

Mantis Id	Description
310258	The system does not send RSTs to DNS server under some L7 DNS TCP floods (DNS Query/Src, DNS Packet - Track/Src). Sources will be blocked if configured. It is unlikely that Source Blocking is used for DNS and also unlikely that there will be TCP-based floods which require a real connection.
354467	For TCP and UDP Port graphs, if a port shows zero traffic for a long period of time and then some traffic arrives, the port graph may show the most recent traffic across the zero-traffic period.
388763	On multi-TP2 models, traffic with Ethertypes 0x9100 (QinQ) and 0x88a8 (802.1ad/aq) is not load-balanced across more than 1 TP2. Ethertype 0x8100 (802.1q) works as expected.
390662	NTP Server address string (FQDN and/or IP addresses) is not validated. Use care when entering.
397103	The default all-route IPv6 address - ::/0 - does not result in IPv6 blocking when entered in a Global ACL.
400781	During very heavy attacks the Executive Summary > DDoS Attack Log graph page may become unresponsive. So far, this has only been observed in the lab.
404557	The system allows duplicate IP addresses or IP/subnet masks between Global and SPP Address Config. Global ACLs will take precedence.
404713	In Time Zone settings under System > Maintenance, some city-pairs are not matching the correct time zone. Set the time zone based on the correct GMT offset for non-daylight-savings time.
411833	Report schedule hour configuration does not adjust for Daylight Savings Time change. For example, if reports are scheduled to run at 9:00 am, they will run at 10:00 am after time change.
413984	No HTTPS Server certificate is displayed and a certificate needs to be selected before any changes can be made on the System > Admin > Settings tab.
415244	Boot Alternate Firmware button should not be used. This option will be removed in future releases.
436137	No validation is done on IP/Domain Reputation User name/Password entries.

Mantis Id	Description
439122	Event Remote Log allows duplicate entries. Care should be taken to avoid entering duplicates.
439204	Editing an existing entry to an invalid string in Admin/Radius/LDAP Trusted hosts, clears the original value.
439530	When Global ACL list exceeds 8192 entries, the GUI may not react to additional feature settings for the ACL item.
439549	Remote Log entry IP address is not validated by the system.
439712	SPP ID numbers are not validated when entered via CLI. User should take care to avoid duplicates if working in CLI.
439960	When there are a very large number of connections, Diagnostic > Sessions/Sources page may not be current.
440143	SNMPv3 options are not exactly the same for Traps and Queries.
442245	Under some conditions, users with RADIUS authentication may not have access to all SPPs.
442830	If the system is in Wire Mode link synchronization and one link has failed, (resulting in second link being failed by the system) a reboot will lose that link synchronization. On reboot, the failed link will not be reflected to the second link.
443933	IP addresses added to Extended Timeout Policy are not validated against other possible entries (ACLs, SPP Policies, etc.). Add these entries with care. For example, if the same IP is entered in ACL Deny policy, and as Extended Timeout Policy, that IP will be Denied.
444070	In testing, Port Statistics and SPP Statistics graphs may not match exactly due to data collection timing. 4.4.0 and 4.5.0 release improves this and we do not think this will affect real-world information.
444593	Modifying a Geolocation ACL may not modify the ACL tables. Add and delete Geolocation ACLs rather than modifying the existing ACLs.
464136	If you delete any report while generating a large number of reports, the GUI may lose contact with the system and get locked. Reloading the page and re-login may be necessary.
467210	During system configuration restore, errors might result in partial configurations. Customer should check configuration once restored to ensure all items are restored.
469829	Changing from user-installed certificate to factory certificate may lock the GUI. Close and re-open browser to restore the GUI.

Mantis Id	Description
471088	A very large SPP configuration may timeout while doing an SPP Restore via GUI, resulting in a partial configuration. Check your configuration once complete and restore via CLI if this problem is experienced. This problem has not been reported from the field.
471157	If a TCP port is configured as a Global Service Port, thresholds cannot be set for that port in any SPP. This was design-intent but will be changed in a future release.
473089	If you leave pages with progress meters, while they are actively displaying progress, when you return, the progress information is lost. Examples are Factory Reset and Generate Traffic Statistics.
477303	If the system has both trusted hosts and RADIUS trusted hosts, the standalone trusted hosts will have precedence.
478130	Event Log entries for Domain Blacklist and Domain Reputation changes are the same and may appear to be duplicates under some conditions.
489669	If the system fails to change Slave configuration in HA setup, occasionally it will report 'Success' message. In worst case, the Slave will eventually notice a database mismatch and reboot to get the entire database.
492991	Attack Log SQL database backup will not work on Slave HA system. The system needs to be changed to Standalone, backup taken and then returned to HA mode. Attack Log **can** be saved as CSV from Slave at any time.
519240	When upgrading an HA pair, HA Group, ID and Priority are removed from the configuration on both systems.
520901	If more than one Threshold-based Report is created, only the last one runs on a Threshold violation.
439530 440064	When Global ACL list exceeds 8192 entries, the GUI may not react to additional feature settings for the ACL item.
520904 520898	Customers are reporting that Threshold-based reports are running when Scheduled Reports run or are generated randomly.
531378	Rarely, under heavy traffic lab conditions, Sources may not age properly from the Source tables, resulting in Hash and/or Memory drops.