DDoS Attack Mitigation

FortiDDoS™ 4.1.11

Release Notes

FortiDDoS™ 4.1.11 Release Notes for B Series Models

January 27, 2016

Revision 1

Technical Documentation	http://docs.fortinet.com
Knowledge Base	http://kb.fortinet.com
Forums	https://support.fortinet.com/forums
Customer Service & Support	https://support.fortinet.com
Training	http://training.fortinet.com
FortiGuard Threat Research & Response	http://www.fortiguard.com
License Agreement	http://www.fortinet.com/doc/legal/EULA.pdf
Document Feedback	Email: techdocs@fortinet.com

Table of contents

Introduction

This document provides a list of new/changed features, upgrade instructions and caveats, resolved issues, and known issues for FortiDDoS 4.1.11, build 0174. The TP2ASIC version is: 410a0065 Date: Dec 30, 2015.

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

Bug fixes only.

Hardware support

This release supports the following hardware models:

- FortiDDoS 200B
- FortiDDoS 400B
- FortiDDoS 600B
- FortiDDoS 800B
- FortiDDoS 900B
- FortiDDoS 1000B
- FortiDDoS 1000B-DC
- FortiDDoS 1200B
- FortiDDoS 2000B
- FortiDDoS 2000B-USG

FortiDDoS A series models are not supported.

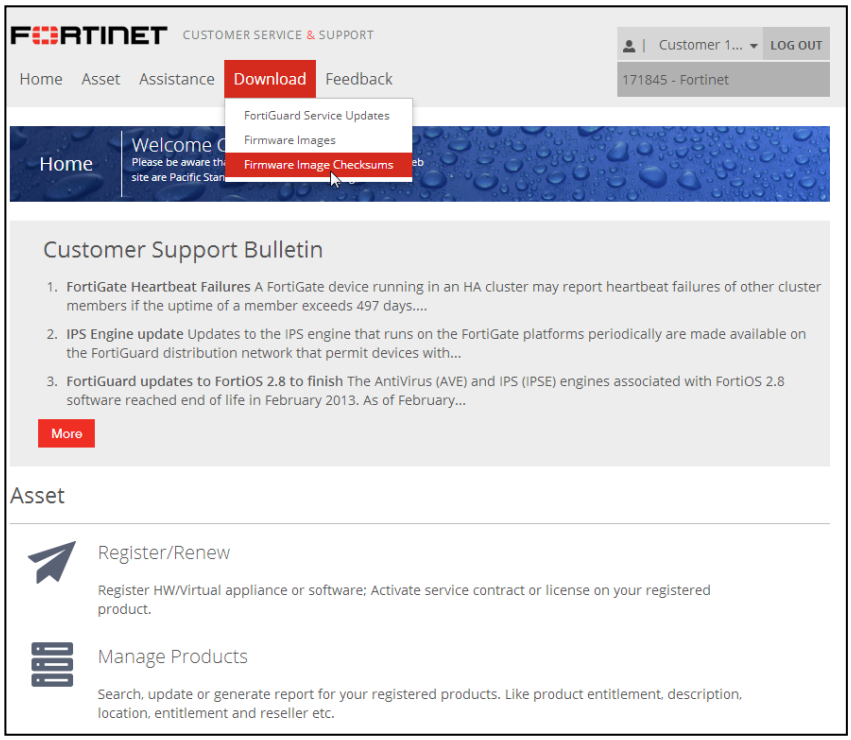
Image checksums

To verify the integrity of the firmware file, use a checksum tool to compute the firmware file's MD5 checksum. Compare it with the checksum indicated by Fortinet. If the checksums match, the file is intact.

MD5 checksums for software releases are available from Fortinet Customer Service & Support:

https://support.fortinet.com

Figure 1: Customer Service & Support image checksum tool



After logging in to the web site, in the menus at the top of the page, click **Download**, and then click **Firmware Image Checksums**.

Alternatively, near the bottom of the page, click the **Firmware Image Checksums** button. (The button appears only if one or more of your devices have a current support contract.) In the Image File Name field, enter the firmware image file name including its extension, then click **Get Checksum Code**.

Upgrading

Use the following instructions to upgrade to 4.1.11.

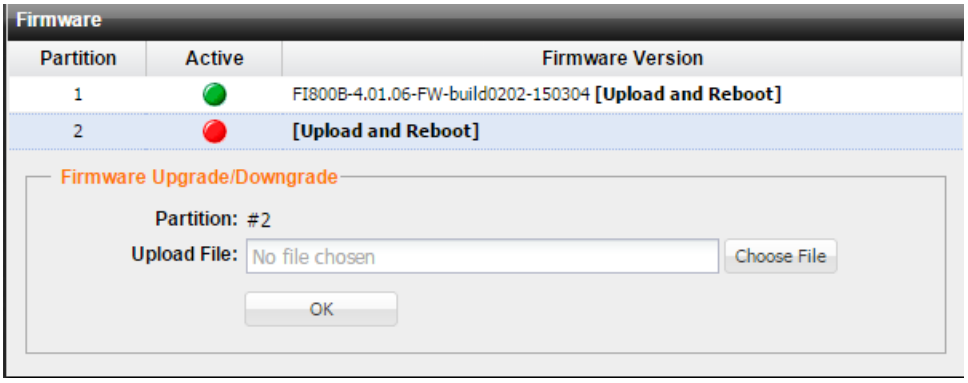
Supported upgrade paths

From 4.1.5 or later	Upgrade directly using the web UI or CLI. Follow the procedure in Section 1 or Section 2 below.
From 4.1.4 or earlier	**1.** Upgrade to 4.1.5. You must use BIOS option G to copy the 4.1.5 image from a TFTP server. Follow the procedure in Section 3 below. **2.** Then, upgrade to 4.1.11 using the web UI or CLI. Follow the procedure in Section 1 or Section 2 below.
From 4.0.x	**1.** Upgrade to 4.1.5. You must use two BIOS options: Option F to format the boot device and then option G to copy the 4.1.5 image from a TFTP server. Follow the procedure in Section 4 below. **2.** Then upgrade to 4.1.11 using the web UI or CLI. Follow the procedure in Section 1 or Section 2 below.

Section 1: Upgrading from 4.1.5 and later with the web UI

You can use the web UI to upgrade from 4.1.5 and later.

The following figure shows the user interface for managing firmware. For this upgrade, you must use Partition 2.



Before you begin:

- Direct upgrade is supported only from 4.1.5 and later. If you have not already done so, upgrade to 4.1.5 using the procedures provided.
- Download the firmware file from the Fortinet Technical Support website: https://support.fortinet.com/

- Back up your configuration before beginning this procedure. If you later revert to an earlier firmware version, the active configuration is deleted, and you will want to restore the configuration that worked well with the earlier version.
- Make a note of configurations that are disabled in your active configuration. Configurations that are not enabled are not preserved in the upgrade to 4.1.11. For example, if a custom HTTP service port, log remote port, or event log port have been configured and then disabled in an earlier version, the port information is not preserved in the upgrade to 4.1.11.
- Make a note of threshold configurations that have been manually set (thresholds that are not named "sys_reco...."). Do this for all SPPs. Improvements have been made to the system recommended thresholds. After you upgrade, you will regenerate system recommended thresholds, and you must re-enter your manual threshold settings.
- You must have super user permission (user admin) to upgrade firmware.

To install firmware:

1. Go to System > Maintenance > Backup & Restore.
2. Under Firmware Upgrade/Downgrade, in the row for Partition 2, click **Upload and Reboot** to display the upload file controls.
3. Use the upload file controls to select the firmware image file.
4. Click **OK** to upload the file, install the firmware, and restart the system. The reboot takes a few minutes but there is no progress indicator.
5. Clear your browser cache to avoid potential issues that can be caused by caching.

Note: Release 4.1.8 included improvements to system recommended thresholds. If you already upgraded to 4.1.8, you do not need to reset your baseline thresholds. If your upgrade path is from a release prior to 4.1.8, take the following additional steps after the upgrade to 4.1.11 has completed and the system has restarted:

1. For each SPP, immediately go to Protection Profiles > Traffic Statistics > Generate and generate statistics for the longest known period with no major attack traffic (8-hours, 1-day, 1-week (recommended), 1-month).
2. Go to Protection Profiles > Thresholds > System Recommendation and set the thresholds based on the generated statistics.
3. Go to Protection Profiles > Thresholds > Thresholds and re-enter the manual threshold settings you want to continue using from your previous configuration.

Section 2: Upgrading from 4.1.5 and later with the CLI

You can use the CLI to upgrade from 4.1.5 and later.

Before you begin:

- Direct upgrade is supported only from 4.1.5 and later. If you have not already done so, upgrade to 4.1.5 using the procedures provided.
- You must be able to use TFTP to transfer the firmware file to the FortiDDoS system. If you do not have a TFTP server, download and install one, like tftpd (Windows, Mac OS X, or Linux), on a server located on the same subnet as the FortiDDoS system.
- Download the firmware file from the Fortinet Technical Support website: https://support.fortinet.com/
- Copy the file to a location you can access from the FortiDDoS appliance using TFTP.
- Back up your configuration before beginning this procedure. If you later revert to an earlier firmware version, the active configuration is deleted, and you will want to restore the configuration that worked well with the earlier version.
- Make a note of configurations that are disabled in your active configuration. Configurations that are not enabled are not preserved in the upgrade to 4.1.11. For example, if a custom HTTP service port, log remote port, or event log port have been configured and then disabled in an earlier version, the port information is not preserved in the upgrade to 4.1.11.
- Make a note of threshold configurations that have been manually set (thresholds that are not named "sys_reco...."). Do this for all SPPs. Improvements have been made to the system recommended thresholds. After you upgrade, you will regenerate system recommended thresholds, and you must re-enter your manual threshold settings.
- You must have super user permission (user admin) to upgrade firmware.

To install firmware:

1. Connect your management computer to the FortiDDoS console port using an RJ-45-to-DB-9 serial cable or a null-modem cable. Use the following terminal settings:

   Speed (Baud Rate): 9600 Data Bits: 8 Stop Bits: 1 Parity: None
2. Initiate a connection to the CLI and log in as the user admin.
3. Use an Ethernet cable to connect FortiDDoS mgmt1 to the TFTP server directly, or connect it to the same subnet as the TFTP server.
4. If necessary, start the TFTP server.
5. Enter the following command to transfer the firmware image to the FortiDDoS system:

   ```
   execute restore image tftp <filename_str> <tftp_ipv4>
   ```

   where <filename_str> is the name of the firmware image file and <tftp_ipv4> is the IP address of the TFTP server. For example, if the firmware image file name is image.out and the IP address of the TFTP server is 192.168.1.168, enter:

   ```
   execute restore image tftp image.out 192.168.1.168
   ```

   The following message appears:

   ```
   This operation will replace the current firmware version!
   Do you want to continue? (y/n)
   ```
6. Type y.

   The system gets the image from the TFTP server, installs the firmware, and restarts. The reboot takes a few minutes but there is no progress indicator.

```
Connect to tftp server 192.168.1.168 ...
Please wait...
#########################################################################
####
Get image from tftp server OK.
Verifying the integrity of the firmware image.
FI900BXXXXXXXXX #

The system begins to upgrade ...


Firmware upgrade in progress ...
New image: FI900B-4.01.11-FW- build0174,160126
Done. 2


The system is going down NOW !!

Please stand by while rebooting the system.
FortiDDoS-900B (15:31-08.24.2015)
Ver:05000001
Serial number:FI900BXXXXXXXXX
RAM activation
CPU(00:000206d7 bfebfbff): MP initialization
CPU(01:000206d7 bfebfbff): MP initialization
CPU(02:000206d7 bfebfbff): MP initialization
CPU(03:000206d7 bfebfbff): MP initialization
CPU(04:000206d7 bfebfbff): MP initialization
CPU(05:000206d7 bfebfbff): MP initialization
CPU(06:000206d7 bfebfbff): MP initialization
CPU(07:000206d7 bfebfbff): MP initialization
CPU(08:000206d7 bfebfbff): MP initialization
CPU(09:000206d7 bfebfbff): MP initialization
CPU(0a:000206d7 bfebfbff): MP initialization
CPU(0b:000206d7 bfebfbff): MP initialization
Total RAM: 32768MB
Enabling cache...Done.
Scanning PCI bus...Done.
Allocating PCI resources...Done.
Enabling PCI resources...Done.
Zeroing IRQ settings...Done.
Verifying PIRQ tables...Done.
Boot up, boot device capacity: 15272MB.
Press any key to display configuration menu...
......

Reading boot image 2791175 bytes.
Initializing FortiDDoS...


System is started.

FortiASIC-TP.0: update started. Reconfigure process takes a few
minutes
FortiASIC-TP.1:   0% Complete
FortiASIC-TP.0:   0% Complete
FortiASIC-TP.2:  10% Complete
```

```
FortiASIC-TP.1:  10% Complete
FortiASIC-TP.0:  10% Complete
FortiASIC-TP.2:  20% Complete
FortiASIC-TP.1:  20% Complete
FortiASIC-TP.0:  20% Complete
FortiASIC-TP.2:  30% Complete
FortiASIC-TP.1:  30% Complete
FortiASIC-TP.0:  30% Complete
FortiASIC-TP.2:  40% Complete
FortiASIC-TP.1:  40% Complete
FortiASIC-TP.0:  40% Complete
FortiASIC-TP.2:  50% Complete
FortiASIC-TP.1:  50% Complete
FortiASIC-TP.0:  50% Complete
FortiASIC-TP.2:  60% Complete
FortiASIC-TP.1:  60% Complete
FortiASIC-TP.0:  60% Complete
FortiASIC-TP.2:  70% Complete
FortiASIC-TP.1:  70% Complete
FortiASIC-TP.0:  70% Complete
FortiASIC-TP.2:  80% Complete
FortiASIC-TP.1:  80% Complete
FortiASIC-TP.0:  80% Complete
FortiASIC-TP.2:  90% Complete
FortiASIC-TP.1:  90% Complete
FortiASIC-TP.0:  90% Complete
FortiASIC-TP.2: download complete.
FortiASIC-TP.2: update success (253.225136 s).
FortiASIC-TP.2: chip reconfigure, try again
FortiASIC-TP.1: download complete.
FortiASIC-TP.1: update success (254.154819 s).
FortiASIC-TP.1: chip reconfigure, try again
FortiASIC-TP.2: chip reconfigure... success.
FortiASIC-TP.1: chip reconfigure... success.
FortiASIC-TP.0: download complete.
FortiASIC-TP.0: update success (257.634973 s).
FortiASIC-TP.0: chip reconfigure, try again
FortiASIC-TP.0: chip reconfigure... success.
FortiASIC-TP.0: update finished
FortiASIC-TP.1: update finished
FortiASIC-TP.2: update finished
rebooting
FortiDDoS-900B (15:31-08.24.2015)
Ver:05000001
Serial number:FI900BXXXXXXXXX
RAM activation
CPU(00:000206d7 bfebfbff): MP initialization
CPU(01:000206d7 bfebfbff): MP initialization
CPU(02:000206d7 bfebfbff): MP initialization
CPU(03:000206d7 bfebfbff): MP initialization
CPU(04:000206d7 bfebfbff): MP initialization
CPU(05:000206d7 bfebfbff): MP initialization
CPU(06:000206d7 bfebfbff): MP initialization
CPU(07:000206d7 bfebfbff): MP initialization
CPU(08:000206d7 bfebfbff): MP initialization
CPU(09:000206d7 bfebfbff): MP initialization
CPU(0a:000206d7 bfebfbff): MP initialization
CPU(0b:000206d7 bfebfbff): MP initialization
Total RAM: 32768MB
```

```
Enabling cache...Done.
Scanning PCI bus...Done.
Allocating PCI resources...Done.
Enabling PCI resources...Done.
Zeroing IRQ settings...Done.
Verifying PIRQ tables...Done.
Boot up, boot device capacity: 15272MB.
Press any key to display configuration menu...
......

Reading boot image 2791175 bytes.
Initializing FortiDDoS...


System is started.
```

To verify that the firmware was successfully installed, login and use the get system status command:

```
FI900BXXXXXXXXX login: admin
Password:
Welcome!

FI900BXXXXXXXXX # get sy st
Version:            FortiDDoS-900B v4.1.11,build0174,160126
TP2ASIC Version:    410a0065 Date: Dec 30, 2015
IP Reputation DB:   Not enabled
Serial-Number:      FI900BXXXXXXXXX
BIOS version:       05000001
Log disk:           Capacity 62 GB, Used 214 MB ( 0.34%), Free 62 GB
RRD disk:           Capacity 369 GB, Used 163 GB (44.20%), Free 206
GB
Hostname:           FI900BXXXXXXXXX
HA configured mode: standalone
HA effective mode:  standalone
Distribution:       International
License Type:       -
Uptime:             0 days  0 hours  13 minutes
Last reboot:        Thu Nov 10 08:07:07 PDT 2015
System time:        Thu Nov 10 08:20:08 PDT 2015
```

Note: Release 4.1.8 included improvements to system recommended thresholds. If you already upgraded to 4.1.8, you do not need to reset your baseline thresholds. If your upgrade path is from a release prior to 4.1.8, take the following additional steps after the upgrade to 4.1.11 has completed and the system has restarted:

1. For each SPP, immediately go to Protection Profiles > Traffic Statistics > Generate and generate statistics for the longest known period with no major attack traffic (8-hours, 1-day, 1-week (recommended), 1-month).
2. Go to Protection Profiles > Thresholds > System Recommendation and set the thresholds based on the generated statistics.

3. Go to Protection Profiles > Thresholds > Thresholds and re-enter the manual threshold settings you want to continue using from your previous configuration.

Section 3: Upgrading from 4.1.x to 4.1.5

You must be on version 4.1.5 or later to upgrade to 4.1.11. Use the following steps to upgrade from earlier versions of 4.1.x to 4.1.5. Steps for upgrading from 4.0.x version are provided below. Upgrade from FortiDDoS 3.x is not supported.

Important: This upgrade removes the existing configuration files from the system. If you want to avoid re-configuring the system, ***follow the instructions in step 1 carefully***. These instructions save and modify the configuration file so that you can restore it later.

This upgrade process preserves your traffic history.

1. Optional. If you want to maintain your configuration across the firmware upgrade:
   a. Use System > Maintenance > Backup & Restore to save your current configuration and then save the backup file as a .txt file.

   For example:

   `FDD-FI400BXXXXXXXXX-2015-05-15.txt`

   b. Open the configuration file in a text editor and make the configuration changes that are required for this upgrade:
      i. In the first line of the configuration, change `FI<model>-4.01.00` to `FI<model>-4.01.05`, where `<model>` is the model number of the appliance that you are upgrading.

      For example, change the following first line:

```
# config-version=FI-2KB-4.01.00-FW-build0141-140404 content:6-0-0
```

      to

```
# config-version=FI-2KB-4.01.05-FW-build0151-141230 content:6-0-0
```

2. Upgrade the firmware:
   a. Download the new firmware image. Contact the Advanced Technology SEs or Customer Support to get this firmware. It is not on the FortiCare download site.
   b. Copy the file to a location you can access from the FortiDDOS appliance using TFTP.
   c. Connect to the FortiDDOS appliance console.
   d. Reboot the system and, when prompted, press any key to display the BIOS configuration menu.
   e. Select option G so that the system can get the new firmware image from the TFTP server and load it when it reboots.

   The following example shows the CLI sequence:

```
FI800BXXXXXXXXX # exe reboot
This operation will reboot the system !
Do you want to continue? (y/n) y
System is rebooting...
The system is going down NOW !!
Please stand by while rebooting the system.
FortiDDoS-800B (19:35-09.19.2013)
Ver:04000005
Serial number:FI800BXXXXXXXXX
```

```
RAM activation
CPU(00:000306a9 bfebfbff): MP initialization
CPU(01:000306a9 bfebfbff): MP initialization
CPU(02:000306a9 bfebfbff): MP initialization
CPU(03:000306a9 bfebfbff): MP initialization
CPU(04:000306a9 bfebfbff): MP initialization
CPU(05:000306a9 bfebfbff): MP initialization
CPU(06:000306a9 bfebfbff): MP initialization
CPU(07:000306a9 bfebfbff): MP initialization
Total RAM: 8192MB
Enabling cache...Done.
Scanning PCI bus...Done.
Allocating PCI resources...Done.
Enabling PCI resources...Done.
Zeroing IRQ settings...Done.
Verifying PIRQ tables...Done.
Boot up, boot device capacity: 15272MB.
Press any key to display configuration menu...
...
[G]:  Get firmware image from TFTP server.
[F]:  Format boot device.
[B]:  Boot with backup firmware and set as default.
[I]:  Configuration and information.
[Q]:  Quit menu and continue to boot with default firmware.
[H]:  Display this list of options.

Enter Selection [G]:

Please connect TFTP server to Ethernet port "MGMT".

Enter TFTP server address [192.168.1.168]: 192.168.1.168
Enter local address [192.168.1.188]: 192.168.1.188
Enter firmware image file name [image.out]: FDD_800B-v400-build0151-
FORTINET.out

MAC:085B0E9F061C

#########################################################################
####

Total 76694566 bytes data downloaded.

Verifying the integrity of the firmware image.


Total 204800kB unzipped.

Save as Default firmware/Backup firmware/Run image without
saving:[D/B/R]?d

Programming the boot device now.

.............................................................
.............................................................
.....................................................

Reading boot image 2791231 bytes.

Initializing FortiDDoS..
```

```
System is started.
```

3. Set the management port IP address and gateway IP address using the console.
4. If you saved and edited the configuration file, restore it using the CLI or web UI.
5. If you did not save a configuration file, you must reconfigure the user accounts and system options.

Section 4: Upgrading from 4.0.x to 4.1.5

You must be on version 4.1.5 or later to upgrade to 4.1.11. Use the following steps to upgrade from 4.0.x to 4.1.5. Upgrade from FortiDDoS 3.x is not supported.

Important: This upgrade removes the existing configuration files from the system. If you want to avoid re-configuring the system, ***follow the instructions in step 1 carefully***. These instructions save and modify the configuration file so that you can restore it later.

This upgrade process preserves your traffic history.

1. Optional. If you want to maintain your configuration across the firmware upgrade:
   a. Document and then delete any ICMP Type/Code service items and any SPP ACLs that use them.

      The syntax for this type of service has changed. You must re-enter these services after you upgrade.

   b. Use System > Maintenance > Backup & Restore to save your current configuration and then save the backup file as a .txt file.

      For example:

      `FDD-FI400BXXXXXXXXX-2015-05-15.txt`

   c. Open the configuration file in a text editor and make the configuration changes that are required for this upgrade:

      i. In the first line of the configuration, change `FI<model>-4.00.01` or `FI<model>-4.00.00` to `FI<model>-4.01.05`, where `<model>` is the model number of the appliance that you are upgrading.

         For example, change the following first line:

```
#config-version=FI400B-4.00.01-FW-build0141-140527 content:6-0-0
```

         to

```
#config-version=FI400B-4.01.05-FW-build0151-141230 content:6-0-0
```

      ii. If you have configured IPv6 dual stack features, locate the section in the .txt file that is similar to the following lines:

```
config ddos global setting
   set ip-v6-dual-stack enable
   set ip-v6-prefix 96
end
```

         Replace the IPv6 prefix settings with the new IPv6 prefix settings. For example, the following lines add settings for an IPv6 network:

```
config ddos global setting
   set ip-v6-prefix-length 64
   set ipv6-prefix 4001:0:0:1::
end
```

iii. If you have configured IPv6 service protection profile (SPP) policies, locate the section in the .txt file that is similar to the following lines:

```
config ddos global spp-policy
   edit subnet1
      set subnet-id 1
      set ipv6 4001:0:0:1::/65
      set spp SPP-0
      next
   end
```

Replace the IPv6 policies with the new IPv6 policies. For example, the following lines add an SPP policy for SPP-0:

```
config ddos global spp-policy
   edit subnet1
      set subnet-id 1
      set ip-version IPv6
      set ipv6 4001:0:0:1::/65
      set spp SPP-0
   next
end
```

Note: When you restore a backup from 4.1.x, IPv4 SPP policies are preserved.

2. Upgrade the firmware:

a. Download the new firmware image. Contact the Advanced Technology SEs or Customer Support to get this firmware. It is not on the FortiCare download site.

b. Copy the file to a location you can access from the FortiDDOS appliance using TFTP.

c. Connect to the FortiDDOS appliance console.

d. Reboot the system and, when prompted, press any key to display the BIOS configuration menu.

e. Select option F to format the boot device.

f. When formatting is complete, select option G so that the system can get the new firmware image from the TFTP server and load it when it reboots.

The following example shows the CLI sequence:

```
FI800BXXXXXXXXX # exe reboot
This operation will reboot the system !
Do you want to continue? (y/n) y
System is rebooting...
The system is going down NOW !!
Please stand by while rebooting the system.
FortiDDoS-800B (19:35-09.19.2013)
Ver:04000005
Serial number:FI800BXXXXXXXXX
RAM activation
CPU(00:000306a9 bfebfbff): MP initialization
CPU(01:000306a9 bfebfbff): MP initialization
CPU(02:000306a9 bfebfbff): MP initialization
CPU(03:000306a9 bfebfbff): MP initialization
CPU(04:000306a9 bfebfbff): MP initialization
CPU(05:000306a9 bfebfbff): MP initialization
CPU(06:000306a9 bfebfbff): MP initialization
CPU(07:000306a9 bfebfbff): MP initialization
Total RAM: 8192MB
```

```
Enabling cache...Done.
Scanning PCI bus...Done.
Allocating PCI resources...Done.
Enabling PCI resources...Done.
Zeroing IRQ settings...Done.
Verifying PIRQ tables...Done.
Boot up, boot device capacity: 15272MB.
Press any key to display configuration menu...
...
[G]:  Get firmware image from TFTP server.
[F]:  Format boot device.
[B]:  Boot with backup firmware and set as default.
[I]:  Configuration and information.
[Q]:  Quit menu and continue to boot with default firmware.
[H]:  Display this list of options.

Enter Selection [F]:

It will erase data in boot device. Continue? [yes/no]: yes

Formatting .......Done.

...
...
[G]:  Get firmware image from TFTP server.
[F]:  Format boot device.
[B]:  Boot with backup firmware and set as default.
[I]:  Configuration and information.
[Q]:  Quit menu and continue to boot with default firmware.
[H]:  Display this list of options.

Enter Selection [G]:

Please connect TFTP server to Ethernet port "MGMT".

Enter TFTP server address [192.168.1.168]: 192.168.1.168
Enter local address [192.168.1.188]: 192.168.1.188
Enter firmware image file name [image.out]: FDD_800B-v400-build0151-
FORTINET.out

MAC:085B0E9F061C

#########################################################################
####

Total 76694566 bytes data downloaded.

Verifying the integrity of the firmware image.


Total 204800kB unzipped.

Save as Default firmware/Backup firmware/Run image without
saving:[D/B/R]?d

Programming the boot device now.

.....................................................................
.....................................................................
.....................................................

Reading boot image 2791231 bytes.
```

```
Initializing FortiDDoS...

System is started.
```

3. Set the management port IP address and gateway IP address using the console.
4. If you saved and edited the configuration file, restore it using the CLI or web UI.
5. Re-enter any ICMP Type/Code services and SPP ACLs that you deleted in the earlier step.

Important: In FortiDDoS 4.1, the system recommended thresholds are determined differently from previous firmware versions. After you upgrade to 4.1, Fortinet recommends that you regenerate traffic statistics and then review and reset the thresholds using Protection Profiles > Thresholds > System Recommendation.

Resolved issues

The following list of issues does not include every bug corrected with this release. For inquires about a particular bug, please contact Fortinet Customer Service & Support.

Table 2: Resolved issues

Bug ID	Description
302401	Upgraded SSL module for web UI server to OpenSSL 1.0.1q pursuant to OpenSSL Security Advisory 20151203.
307574	System "maintainer" account has been removed.

Known issues

The following list of issues for this release is not complete. For inquires about a particular bug, please contact Fortinet Customer Service & Support.

Table 3: Known issues

Bug ID	Description

305299	The system hangs during bootup when you execute the `execute restore config` command after you have executed the `execute formatlogdisk` command, if the configuration file includes commands that require a reboot.
	To work around this issue, remove the commands that require reboot from the configuration file before restoring it, or unset them before backing up a configuration that will later be restored. The commands that require reboot include:
	• timezone (under System->Maintenance->System Time)
	• NTP server (under System->Maintenance->System Time)
	• Tap mode (under Global Settings-> Settings->Settings)
	Before you restore a configuration, ensure the configuration commands like the ones in the following example are not present in the configuration file that will be restored:
	`config system time manual`
	`  set zone 30`
	`end`
	`config system time ntp`
	`  set ntpsync enable`
	`  set ntpserver times.windows.com`
	`end`
	`config ddos global setting`
	` set tap-mode enable`
	`end`

246209	Upgrade from 4.0.x to 4.1.5 cannot be performed with the web UI. Upgrade from 4.1.5 can be performed with the Web UI.

260686	The link status reported in the web UI is the detected link state. This is working as designed. The link status shown in the `show system interface` and `get system interface` configuration commands is the configured status. This is also working as designed.
	To display the detected link state with the CLI, use the following command:
	`FI-2K# diagnose hardware get deviceinfo data-port`
	`port1  down  10G FD  SW  No  Forward  TX RX  None  F  XGMII 16356`
	`port2  down  10G FD  SW  No  Forward  TX RX  None  F  XGMII 16356`
	`port3  down  10G FD  SW  No  Forward  TX RX  None  F  XGMII 16356`

275873	Layer 7 SIP thresholds and graphs are not working correctly and have been removed.
276626	The web UI allows invalid blank URLs and URLs with white spaces to be added.
277768	Triple-tagged VLAN packets will bypass in Detection or Prevention mode. Triple-tagged VLAN packets are unlikely to be seen in deployments outside the firewall.
278358	When a source is blocked due to a Connection/Source flood, the source IP address is not reported in the DDoS Attack log.
278363 278050	Connection/Source and Slow Connection events might not show destination IP addresses in logs, graphs, or traps if the drop count is very small.
278709	If Global Settings > Settings > Drop HTTP Range Header is enabled, Header Range anomalies are dropped but are not shown in logs and graphs.
279751	A very small number of reported drops for SYN/destination, ACK/destination, FIN/destination or RST/destination might get "stuck" in the database and repeat.

284420	When the system is very busy, some Destination IPs might be incorrectly reported in logs.
290403	In DDoS Attack logs: The protocol is incorrectly reported as 0/ip.