FortiBridge - Administration Guide

4.0.0

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

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

Monday, February 23, 2015

FortiBridge - Administration Guide

TABLE OF CONTENTS

Change Log **5**
Introduction **6**
Supported Models 6
Before You Begin 6
How this guide is organized 6
Additional Information 6
Product Overview **7**
Introduction 7
Hardware Configurations 7
Modes of Operation 8
Inline Mode **9**
Description 9
Failure Detection and Recovery 10
Heartbeat Probe 10
System Power Failure 10
Recovery 10
Manual Actions 10
State Transitions 10
TAP Mode **12**
Description 12
State Transitions 12
Failure Detection and Recovery 14
System Power Failure 14
Recovery 14
Getting Started **15**
System Settings 15
User and Password 15
Web User 15
Time and date 15
Administrative port settings 16
Changing the host name 16
Configuration Backups 16
Backing up the configuration using the web-based manager 16

Restoring a configuration 16
Restore factory defaults 16
Firmware Upgrades 17
Configuration using GUI Interface 18
Logging In 18
Dashboard Page 18
System 19
System Information 19
Management Port 20
Administrators 20
Probe 20
Settings 20
Notifications 21
CLI Configuration for Inline mode 23
Set Automatic Recovery from Heartbeat Expiry 23
Set Heartbeat Active Mode 23
Set Heartbeat Characteristics 23
Set Heartbeat Expiry State 24
Set Heartbeat Packet Contents 24
Configure FortiGate for Heartbeat Packets 24
CLI Configuration for TAP Mode 26
Set Keep Heartbeat Active Mode 26
Disable Heartbeat Active Mode 26
Set Bypass Mode 26
CLI Configuration for Modules 27
Select the Current Module 27
List the Module Properties 27
Display the Module State 27
Set the Link Speed 28

Change Log

Date	Change Description
2015-01-28	FortiBridge Release 4.0.0
2015-02-02	Fixed the URL in pointers to the CLI reference. Removed content related to link error-testing and get/set_rx_tx_err_mode (which will be supported in the next release).
2015-02-11	Added section on how to configure FortiGate to permit forwarding of the heartbeat packets.
2015-02-23	Correction to Inline mode: if the heartbeat expiry mode is Failcutoff, the segment WILL automatically transition back to Inline when the heartbeats are restored.

Introduction

This guide explains how to get started with the FortiBridge 3000-series products, and describes common configuration tasks and best practices.

Supported Models

This guide is for all FortiBridge models:

- FBG-3002S (short-range) and FBG-3002L (long-range) - chassis plus one 1G/10G module.
- FBG-3004S (short-range) and FBG-3004L (long-range) - chassis plus two 1G/10G modules.
- FBG-3041S (short-range) - chassis plus one 40G module.

Before You Begin

Before you start administrating your FortiBridge product, you must complete the installation, including configuration of the management port, as outlined in the QuickStart Guide.

How this guide is organized

This guide contains the following sections:

- Product Overview
- Inline Mode
- TAP Mode
- Getting Started
- Configuration using GUI Interface
- CLI Configuration for Inline mode
- CLI Configuration for TAP mode
- CLI Configuration for Modules

Additional Information

For more information about the CLI commands, see the FortiBridge CLI Reference at:

http://docs.fortinet.com/fortibridge/reference

Product Overview

Introduction

FortiBridge enables you to add traffic monitoring and security devices to your network, without any loss in network integrity.

FortiBridge supports two normal modes of operation: inline mode and TAP mode. Inline mode supports network configurations that require in-line monitoring/security devices. TAP mode supports various traffic TAP configurations, where the main network path is mirrored to the monitoring devices.

The FortiBridge product provides monitoring features to ensure that any inline or TAP devices do not impact network integrity and availability. For example, FortiBridge runs a heartbeat probe for in-line configurations, and automatically switches to Bypass mode if the heartbeat fails.

Bypass mode provides active and passive bypass circuitry. Active bypass restores the traffic path between network ports, if the monitoring path fails. If the FortiBridge suffers a catastrophic failure such as power loss, it automatically reverts to Passive Bypass mode, so that traffic flow is not interrupted.

Hardware Configurations

The FortiBridge consists of a host system (a 1U chassis), which houses up to three bypass modules.

A bypass module supports one or more network segments. A network segment provides one inline or bypass traffic path. Each segment provides two network ports (NET0 and NET1) and two monitoring ports (MON1 and MON2).

The following bypass modules are available:

- 40G bypass module
  - Supports one bypass segment.
  - Supports 40G Single mode fiber (40GBase-SR4) network standards
  - Provides MPO/LC ports for the network ports.
  - Provides QSFP+ ports for the monitor ports.
- Dual-rate 1/10G bypass module
  - Supports two bypass segments
  - Supports dual rate 1/10G Multimode Fiber (10GBase-SR , 1000Base-SX) network standards
  - Supports dual rate 1/10G Single mode fiber (10GBase-LR, 1000Base-LX) network standards
  - Provides MPO/LC Duplex ports for the network ports.
  - Provides SFP+ ports for the monitor ports.

The network ports have built-in transceivers. The monitor ports require plug-in optical transceivers. The correct transceivers are delivered (pre-installed) with your FortiBridge product.

Modes of Operation

Each FortiBridge segment operates in one of the following modes:

- Inline mode
  - The system diverts all incoming network traffic to the monitoring ports. No traffic flows directly between the network ports.
  - The inline network element must bridge the traffic between the monitoring ports.
  - The system monitors the inline traffic path using a heartbeat probe.
  - In the event of a fault, the segment transitions to one of the bypass modes (Bypass, TAP or Fail-cutoff mode, depending on configuration values).
  - When the fault condition clears, the segment can automatically transition back to Inline mode (the exact behavior is defined by configuration values). The segment transitions to Inline mode only after it detects that the heartbeat probe is working again
- TAP mode
  - The system sends traffic between the network ports, and incoming traffic is mirrored to the monitoring ports.
  - The system does not provide a heartbeat probe on the mirrored path (because the network path is the primary traffic path).
  - If the system loses power, the traffic path is maintained between the network ports (the segment transitions to passive bypass mode).
- Bypass mode
  - The system sends traffic only between the network ports, and not to the monitoring ports.
- Fail-cutoff mode
  - The system disables the links on the network ports, to simulate cable disconnection between the network devices.

Inline Mode

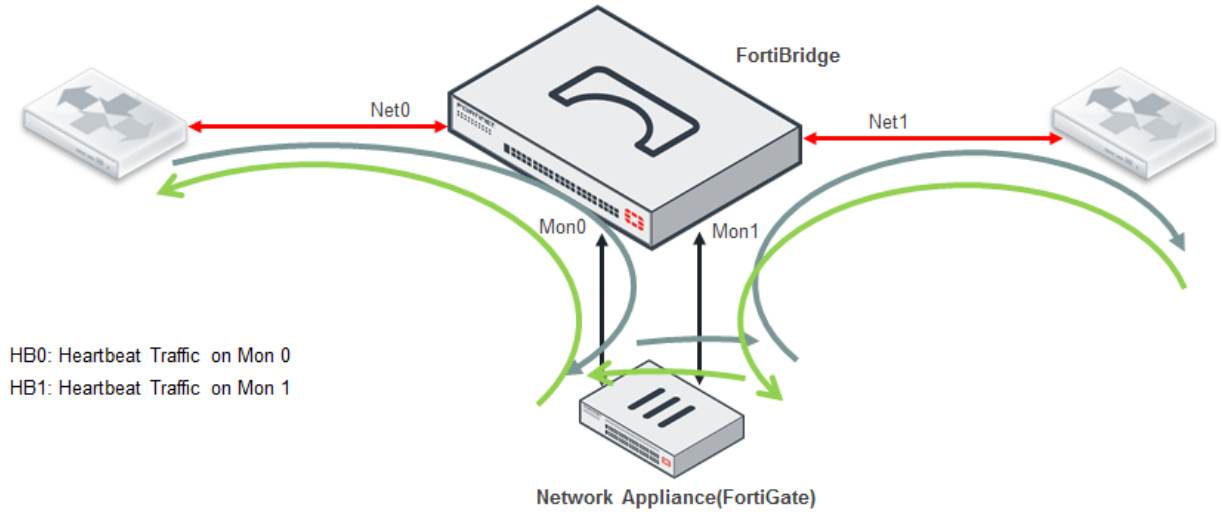
Description

In Inline mode, the FortiBridge segment does not send any traffic directly between the network ports. All incoming traffic from the network ports is diverted to the monitoring ports. The inline network device (connected to the monitoring ports) must bridge the traffic between the monitoring ports.

The inline device can inspect and modify the traffic. Because the device is inline, the network path will be affected by any packet delays or disruptions introduced by the inline device.

You must use Inline mode if the inline network device is intended to alter the traffic (such as discarding packets, rewriting packet headers, etc). Inline mode is suitable for active monitoring of the network traffic, such as security threat detection with response/remediation.

The following diagram shows the packet flow for Inline mode. The grey arrows show traffic flow from left to right (ingress at Net0), and the green arrows show the traffic flow from right to left (ingress at Net1):



Failure Detection and Recovery

FortiBridge provides the following failure detection mechanisms, to ensure that traffic flow through the network is not impacted by a failure in the inline path:

- Heartbeat Probe
- System Power Failure

The following sections provide details about these failure actions and the associated recovery actions for each mechanism.

Heartbeat Probe

The Heartbeat probe ensures that traffic is flowing successfully between the monitoring ports (through the inline network device). The system sends heartbeat packets from the sending monitor port to the inline network device, which bridges the heartbeat packets to the receiving monitor port.

The network segment remains in inline mode as long as it continues to receive the heartbeat packets. You can configure the interval time between heartbeat packets, as well as the maximum time that the segment will wait for a heartbeat packet.

If the heartbeat timer expires before a heartbeat is detected, the system raises the heartbeat expiry event and transitions the segment to one of the bypass modes (Bypass, TAP or Fail-cutoff), depending on the configured value of the heartbeat expiry mode.

System Power Failure

If the FortiBridge experiences a power loss, each network segment transitions to passive bypass mode.

Recovery

By default,the network segment will automatically recover from Bypass, TAP or Fail-cutoff mode to inline mode when it detects that the heartbeat mechanism has been restored. This behavior is configurable.

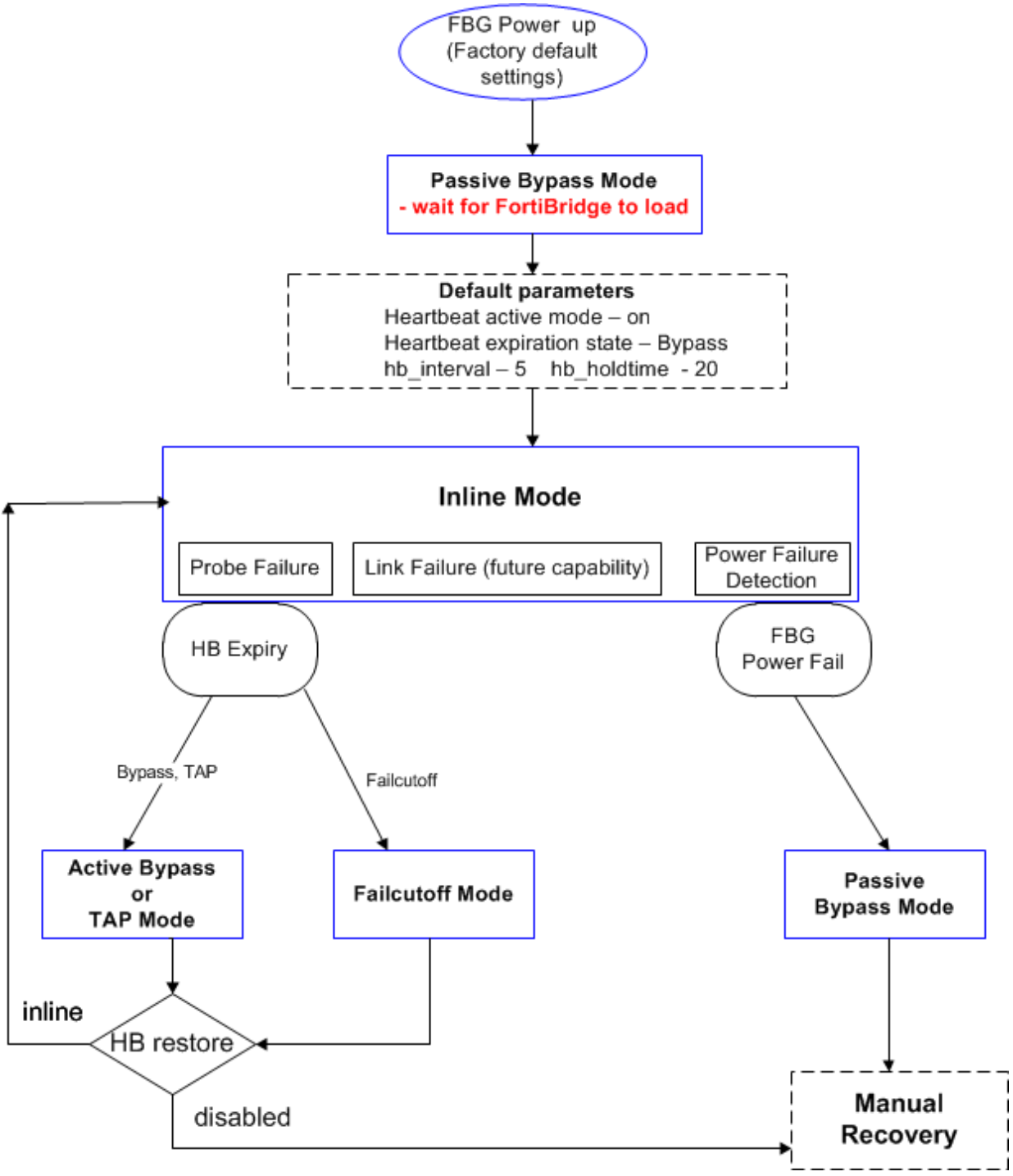
Manual Actions

Using the CLI, you can manually set a segment into bypass, TAP or Fail-cutoff mode.

You can also do a manual restoration to inline mode. With the default configuration, the segment will not stay in inline mode unless the heartbeat probe is running. You can override this behavior using the CLI (set_hb_active disable).

State Transitions

The following diagram illustrates the state transitions that relate to inline mode.


FBG Power up
(Factory default
settings)
Passive Bypass Mode
- wait for FortiBridge to load
Default parameters
Heartbeat active mode – on
Heartbeat expiration state – Bypass
hb_interval – 5 hb_holdtime - 20
Inline Mode
Probe Failure
Link Failure (future capability)
Power Failure
Detection
HB Expiry
FBG
Power Fail
Bypass, TAP
Failcutoff
Active Bypass
or
TAP Mode
Failcutoff Mode
Passive
Bypass Mode
inline
HB restore
disabled
Manual
Recovery

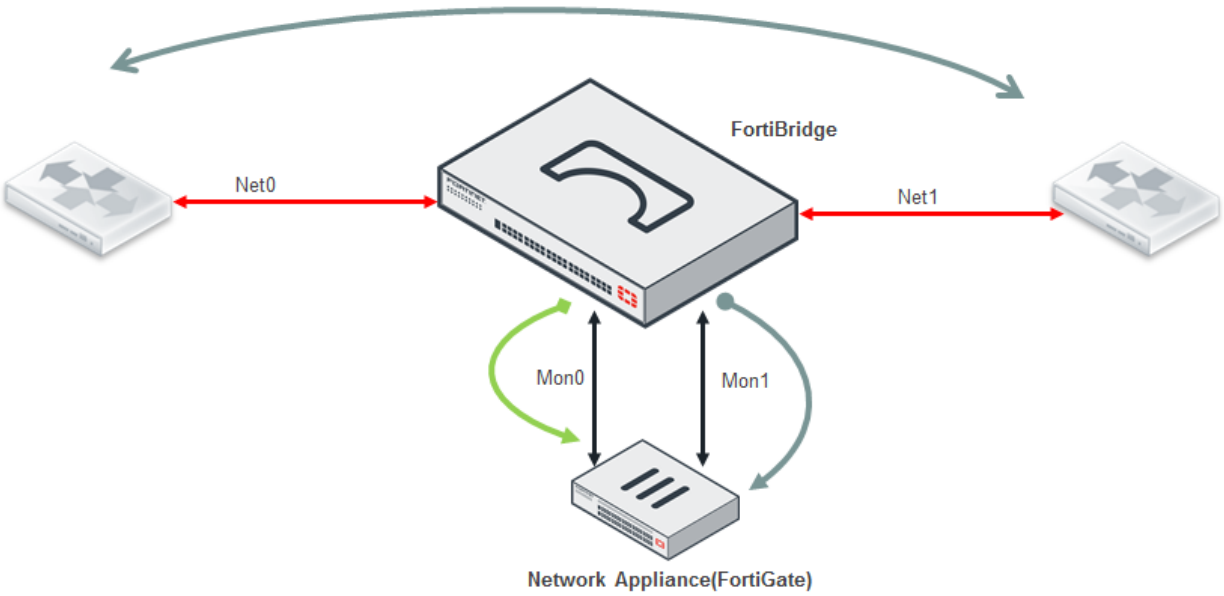
TAP Mode

Description

A network segment in TAP mode will send all traffic between the network ports, and mirror the traffic from the network ports to the monitoring ports. The system provides configuration options that determine the exact mirroring configuration.

A network device connected between the monitoring ports can inspect the traffic without impacting the network. Generally,any changes to the packets will NOT be reflected in the main traffic path (between the network ports).

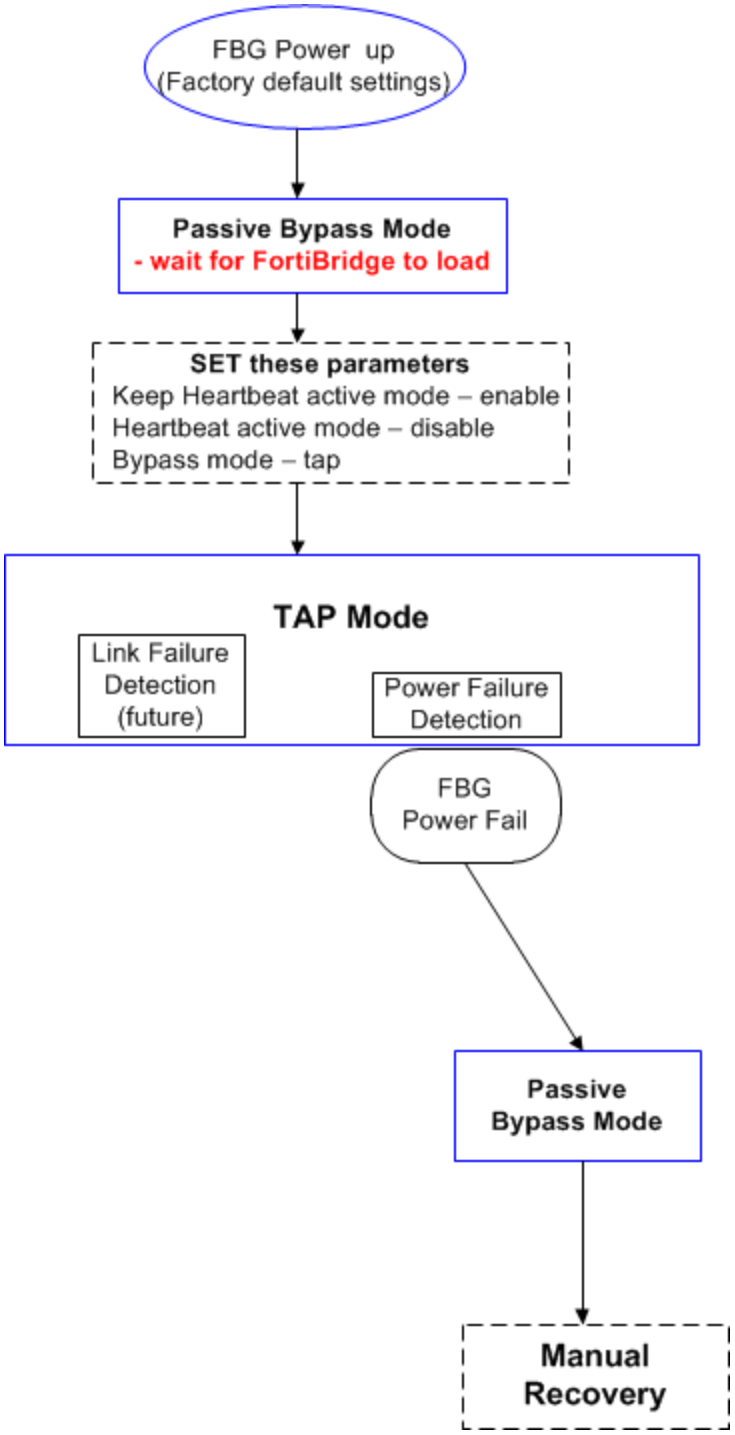
The following diagram shows the packet flow for TAP mode. Traffic flows in both directions between Net0 and Net1. In addition, traffic from Net0 is mirrored to Mon0 and traffic from Net1 is mirrored to Mon1:



The FortiBridge mirrors the incoming traffic from NET0 to MON0 and the incoming traffic from NET1 to MON1

State Transitions

The following diagram illustrates the state transitions that relate to TAP mode.


FBG Power up
(Factory default settings)
Passive Bypass Mode
- wait for FortiBridge to load
SET these parameters
Keep Heartbeat active mode – enable
Heartbeat active mode – disable
Bypass mode – tap
TAP Mode
Link Failure Detection (future)
Power Failure Detection
FBG Power Fail
Passive Bypass Mode
Manual Recovery

Failure Detection and Recovery

There is no heartbeat probe in TAP mode, because a failure in the monitoring path does not impact the main traffic flow (between the network ports).

In TAP mode, the system provides the following failure detection mechanisms:

- System Power Failure

The following sections provide details about these failure actions and the associated recovery actions for each mechanism.

System Power Failure

If the FortiBridge experiences a power loss, each network segment transitions to passive bypass mode.

Recovery

After the failure has been resolved, you must manually transition the segment to TAP mode.

Getting Started

This section contains information about initial CLI configuration tasks that you complete after you have installed the FortiBridge product.

You can connect to the CLI using an SSH or Telnet connection. For connection instructions, refer to the FortiBridge QuickStart Guide. For more information about the CLI, see the FortiBridge CLI Reference Guide at the following location:

http://docs.fortinet.com/fortibridge/reference

System Settings

The following sections describe initial system settings that you should configure before using the product.

User and Password

By default, the administrator account is configured with the username `admin` and no password. In order to prevent unauthorized access to the system, it is highly recommended that you change the user name and password.

To update the admin user and password:

```
FBG-3002L#set_user FBGuser1
FBG-3002L#set_psw
```

The set_psw command will prompt you to enter and confirm the new password. You must log out and then log in again to access the new user account.

Web User

By default, the web account is configured with the username `admin` and no password. In order to prevent unauthorized access to the system, it is highly recommended that you change the user name and password.

To update the web user and password:

```
FBG-3002L#set_web_user FBGuser2
FBG-3002L#set_web_user_psw <old password> <new password>
```

Time and date

You can either manually set the system date and time or configure the system to use a Network Time Protocol (NTP) server. Network Time Protocol enables you to keep the system time in sync with other systems. This will ensure that logs and other time-sensitive settings on the system are correct.

To set the current date and time, using the set_time command (the field order is month, day, hour, minute, and year):

```
FBG-3002L#set_time 2 5 13 10 2010
```

To connect to an NTP server, enable NTP and configure the NTP server address:

```
FBG-3002L#set_ntp_state on
FBG-3002L#set_ntp_server_ip 192.168.2.100
```

Administrative port settings

You can change the IP address, mask and default gateway of the management port, using the following commands:

```
FBG-3002L#set_ip 192.168.2.200 255.255.0.0
FBG-3002L#set_gateway 192.168.2.1
```

Changing the host name

The host name of your system appears at the CLI prompt and as the SNMP system name.

To change the host name, use the set_unit_name command:

```
FBG-3002L#set_unit_name FBG-3002S
```

Configuration Backups

We recommend that you perform a backup of the initial configuration, and after any configuration changes.

If you reset the system to factory defaults or perform a TFTP upload of the firmware, these actions erase the existing configuration.You will need to restore the configuration from a backup.

Store configuration files on the management computer or at an off-site location. You have the option to save the configuration file to a TFTP site.

Backing up the configuration using the web-based manager

1. Go to **System > Status**.
2. On the **Configuration** widget, click **Backup**
3. The web browser will prompt you for a location to save the configuration file. The configuration file will have a .conf extension.

Restoring a configuration

Should you need to restore a configuration file, use the following steps:

1. Go to **System > Status**.
2. On the **Configuration** pull down selector, select the backup file to be restored.
3. click **Restore**.

Restore factory defaults

You may need to reset the system to its original defaults; for example, to begin with a fresh configuration.

You can restore the default values using the CLI by entering the command:

```
FBG-3002L#set_default
```

This command does not reset the speed of the RS-232 management port.

Firmware Upgrades

You can upgrade the system to a newer version of firmware.

1. Copy the new firmware file and the matching 'update.desc' file to the /tftpboot directory of the TFTP server.
2. Enter the following CLI command: `update <tftp server IP address>`
3. When the upgrade is complete, enter the following CLI command: `reboot`

Configuration using GUI Interface

The Administrative GUI Interface is a browser-based tool for configuring and managing the FortiBridge product.

Logging In

To access the GUI Interface:

1. Open a browser window and navigate to the following address: http://192.168.1.99
2. Enter a valid User Name and Password, then click **Login**

After you log in successfully, the system displays the system dashboard page:

Dashboard Page

The system dashboard page displays the system settings and the current status of the system resources (CPU usage and memory usage). To the right of the system settings, the system displays the status of the currently selected module.

The left navigation bar contains links to the following configuration pages.

- **System** - configure the system settings and view system status.
- **Probe** - view and configure probe settings.

The following sections describe these pages.

System

On the left navigational pane, select **System>Status** to display the system settings on the dashboard.

The system dashboard is divided into four panels:

- **System Information** - displays system configuration information. You can change these values.
- **Unit Operation** - displays the status of the selected module. If the current module supports two segments, Unit Operation displays the status of both segments.
- **System Resources** - graphical display of CPU usage and memory usage.
- **Management Port** - displays configuration settings for the management port. You can change these values.
- **Administrators** - displays the user name of the administrator.

System Information

The system information panel displays the current value for each parameter. To change a value, click the associated **Change** link. A pop up window opens, from which you can edit and save the value.

The following table describes the system configuration parameters:

Serial Number	Serial number of the module. This is a read-only field.
Uptime	Elapsed time since this system last started up. This is a read-only field.
System Time	The system time. If NTP is enabled, NTP will override any manual changes.
Host Name	The host name appears at the CLI prompt and as the SNMP system name.
Operation Mode	Displays the mode for the current segment. FortiBridge can automatically transition to the Inline mode (based on configuration settings). You can manually set the mode using this field.
Current Module	The chassis supports up to three modules. If this system is provisioned with more than one module, you can change the value of **Current Module**.
Current Segment	The current segment. If the current module supports more than one segment, you can select a new value for current segment.
Firmware version	Current firmware version. To perform an upgrade, click the **upgrade** button. The system opens a file browser; use the file browser to select a firmware file. The system upgrades using the selected firmware file.
Configuration backup and restore	To create a new backup configuration file, click **Backup** and enter a new file name (or select an existing file, to overwrite this file). To restore the configuration from a file, click **Restore** and then select a filename from the drop-down list.
MAC Address 1	MAC address of the management port

MAC Address 2	MAC address of the MON0 port (for the current segment)
MAC Address 3	MAC address of the MON1 port (for the current segment)

Management Port

You can view or update the following settings for the management port:

IP/Network	The IP address and mask of the management port.
Telnet/SSH	Enable SSH or Telnet.
Default Gateway	The default gateway for the management port.

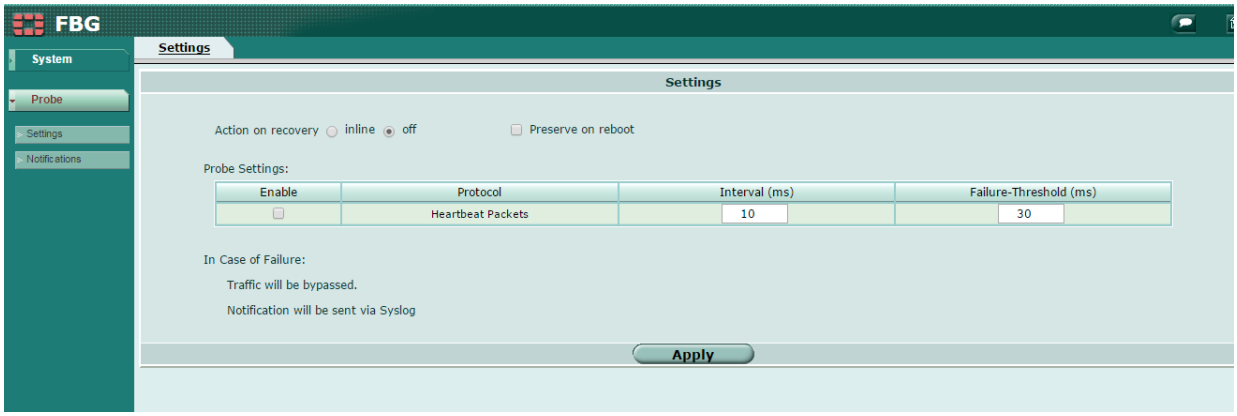
Administrators

Click on the edit button to change the administrator user name or password.

Probe

Use the probe page to view and configure the system probes for the current segment. You can select **Settings** or **Notifications** from the left-panel menu.

Below the list of probes, the system displays the actions that will occur if the probe (for the current segment) reports a failure.



Settings

On the left navigational pane, select **Probe>Settings** to view and configure probe settings.

You can configure the following options related to recovery action (click the Apply button after you change the value):

Action on recovery	inline - the segment will attempt to recover to inline mode after a failure off - the segment will require manual recovery.
Preserve on reboot	If you check this option, the system will preserve the recovery action value across a reboot.

You can configure the following settings for the Heartbeat probe(click the Apply button after you change the value):

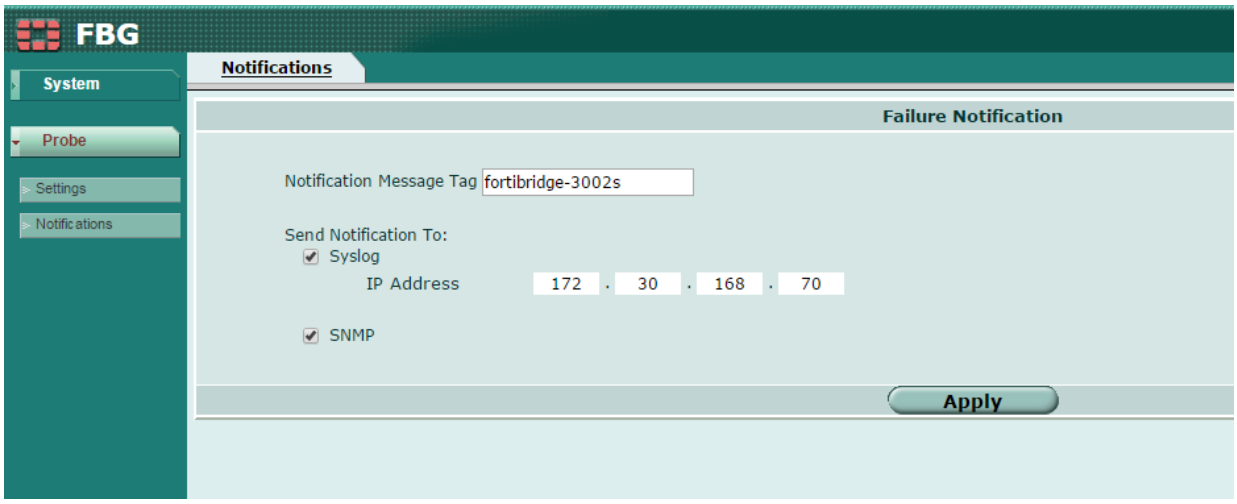
Enable	Enables the heartbeat probe.
Interval	The interval is the frequency with which the sending port sends a heartbeat packet.
Failure Threshold	The failure threshold defines the maximum time that the receiving port will wait for the next heartbeat message. If the heartbeat is not received within this time, the system triggers the heartbeat expiry event.

NOTE: set the failure threshold to a value at least 3 times the interval value.

Notifications

On the left navigational pane, select **Probe>Notifications** to view and configure the choices for communicating probe-detected failures.

The following figure shows the notifications page:



The probe notification fields are described in the following table:

Notification Message Tag	Text tag that the system will add to Syslog entries and SNMP trap entries.
Syslog	Select this option to send notifications to the system log.
IP Address	IP address of the syslog device.
SNMP	Select this option to report notifications using SNMP.

CLI Configuration for Inline mode

This chapter describes the CLI configuration settings related to Inline mode.

With the default configuration values, the system will transition each network segment into Inline mode. To restore a segment to the default inline operation, set the following values:

- Set the current module and segment
- Active heartbeat restore: Inline
- Heartbeat active mode: Enable
- Heartbeat interval: 5
- Heartbeat hold time: 20
- Heartbeat expiry state: Bypass
- (Optional) Define a custom heartbeat packet

The following sections provide information about these parameters.

Set Automatic Recovery from Heartbeat Expiry

FortiBridge supports automatic or manual recovery from heartbeat expiry. The default actions is automatic recovery to Inline mode. You can change the configuration to set manual recovery.

```
FBG-3002L#set_en_act_hb_restore inline
```

Set Heartbeat Active Mode

When heartbeat active mode is enabled,the segment automatically transitions to inline mode.

To set heartbeat active mode:

```
FBG-3002L#set_hb_act_mode enable
```

Set Heartbeat Characteristics

Use these commands to set the heartbeat interval time and hold time.

The heartbeat interval specifies how often the heartbeat packets are generated by the sending port.

The heartbeat hold time specifies the maximum time that the receiving port will wait for a heartbeat packet. If the packet is not received within this time, the system triggers the heartbeat expiry event.

NOTE: set the hold time to be at least 3 times the heartbeat interval.

```
FBG-3002L#set_hb_interval 10
FBG-3002L#set_hb_holdtime 40
```

By default, the heartbeat is sent by Mon0 and received at Mon1. You can reverse the direction of the heartbeat, and you can also set it to be bidirectional, as shown in the following example:

```
FBG-3002L#set_hb_tx_dir bidirectional
```

Set Heartbeat Expiry State

Use this command to set the heartbeat expiry mode for the current segment.

The system will transition this segment to the heartbeat expiry mode if the heartbeat expiry event is detected.

```
FBG-3002L#set_hb_exp_state bypass
```

Set Heartbeat Packet Contents

The system includes a default heartbeat packet format. You can define a custom format for the heartbeat packet, and load it into the system.

Load the Heartbeat contents. The load command expects a file named "'hb.bin".

```
FBG-3002L#load_hb_pkt 192.168.0.2 tftpboot
```

Restore the Heartbeat contents to the default content:

```
FBG-3002L#set_default_hb_pkt
```

See the FortiBridge CLI Reference for additional information about defining a custom heartbeat packet:

http://docs.fortinet.com/fortibridge/reference

Configure FortiGate for Heartbeat Packets

The heartbeat probe relies on the inline network device to pass the heartbeat packets between the two monitor ports. If your inline device is a firewall, you need to configure the firewall ports (that are attached to the monitor ports) to accept and forward the heartbeat packets. For the default heartbeat packet, you also need to enable Layer 2 forwarding.

The following example shows the configuration required for a FortiGate firewall. Port10 and port11 are the Fortigate interfaces that are connected to the Fortibridge monitor ports:

```
config firewall policy
   edit 1
      set srcintf "port10"
      set dstintf "port11"
      set srcaddr "all"
      set dstaddr "all"
      set action accept
      set schedule "always"
      set service "ALL"
   next
```

```
    edit 2
       set srcintf "port11"
       set dstintf "port10"
       set srcaddr "all"
       set dstaddr "all"
       set action accept
       set schedule "always"
       set service "ALL"
    next
end
```

Enable Layer 2 forwarding:

```
config system interface
    edit port10
       set l2forward enable
    edit port11
       set l2forward enable
```

CLI Configuration for TAP Mode

This section describes the configuration tasks required for a network segment to operate in TAP mode.

By default, each network segment will transition to Inline mode. Therefore, you must set the following configuration values for a network segment to transition into TAP mode:

- Set the current module and segment
- Keep Heartbeat active mode: Enable
- Heartbeat active mode: Disable
- Bypass mode: set to TAP mode

Set Keep Heartbeat Active Mode

Set the Keep Heartbeat Active Mode to enabled, so that the Heartbeat Active Mode value will survive a power cycle or restart. If you set this parameter to disabled, the segment will come up in Inline mode.

```
FBG-3002L#set_keep_hb_act_mode enable
```

Disable Heartbeat Active Mode

Set heartbeat active mode to disabled. The segment transitions to the mode configured in Bypass Mode.

```
FBG-3002L#set_hb_act_mode disable
```

Set Bypass Mode

When the heartbeat active mode is set to disabled, the segment transitions to the mode configured in Bypass Mode. Set the value to TAP.

```
FBG-3002L#set_bypass_mode tap
```

CLI Configuration for Modules

The FortiBridge host system houses up to three bypass modules.

A bypass module supports one or more network segments. A network segment provides one inline or bypass traffic path. Each segment provides two network ports (NET0 and NET1) and two monitoring ports (MON1 and MON2).

The available Bypass modules include:

- 40G bypass module
  - Supports one bypass segment.
- Dual-rate 1/10G bypass module
  - Supports two bypass segments
  - Available with short-reach or long-reach optics.

The following sections describe common configuration tasks required for the bypass modules.

Before you start to configure a specific module or segment, you need to set the module and segment as "current", using the set_seg command.

Select the Current Module

Set the module and segment to be current:

```
FBG-3002L#set_seg 1 1
```

Displays the current module and segment :

```
FBG-3002L#get_seg
```

Blinks the S.OK LED on the current module:

```
FBG-3002L#whoami enable
```

List the Module Properties

Displays the settings for each of the installed modules.

```
FBG-3002L#get_dev_prop
```

Display the Module State

Displays information about the state of the current module.

Note: this command resets the Alarm LED.

```
FBG-3002L#get_dev_state
```

Set the Link Speed

The 10G bypass modules support dual-rate link speed (1G or 10G). To set the link speed, use the set_seg_speed command. The command will set the link speed for the current segment. You can specify **all** to set the value for all of the segments on the current module:

```
FBG-3002L#set_seg_speed [all] (auto | 10g | 1g)
```