FortiBridge - Administration Guide

4.3.0

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

Wednesday, March 09, 2016

FortiBridge - Administration Guide

Version 4.3.0

TABLE OF CONTENTS

Change Log

Date	Change Description
2015-01-28	FortiBridge Release 4.0.0
2015-05-01	Updates for FortiBridge Release 4.1.0
2015-05-27	Removed the upgrade instructions for 4.0 to 4.1, and refer the user to the Release Notes to obtain these instructions.
2015-09-16	Started a troubleshooting chapter. Added commands to switch CLI view between 4.0 and 4.1 Clarified the upgrade procedures.
2015-10-02	Updates for FortiBridge Release 4.2.0
2016-03-04	Updates for FortiBridge Release 4.3.0

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 series 3000 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-3004SL (supports short-range and long-range) - provides four 1G/10G network segments.
- FBG-3041S (short-range) - provides one 40G network segment.
- FBG-3042S (short-range) - provides two 40G network segments.

Before You Begin

Before you start to configure and manage 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 Bypass 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 traffic TAP configurations, where the main network path is mirrored to the monitoring devices.

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

In bypass mode, the traffic path runs between the network ports. In active bypass mode, an active circuit directs the traffic path between the network ports (for example, if the monitoring path has failed). If the FortiBridge suffers a catastrophic failure such as power loss, it automatically reverts to Passive Bypass mode - a passive circuit directs the traffic flow between the network ports, so that network traffic 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.

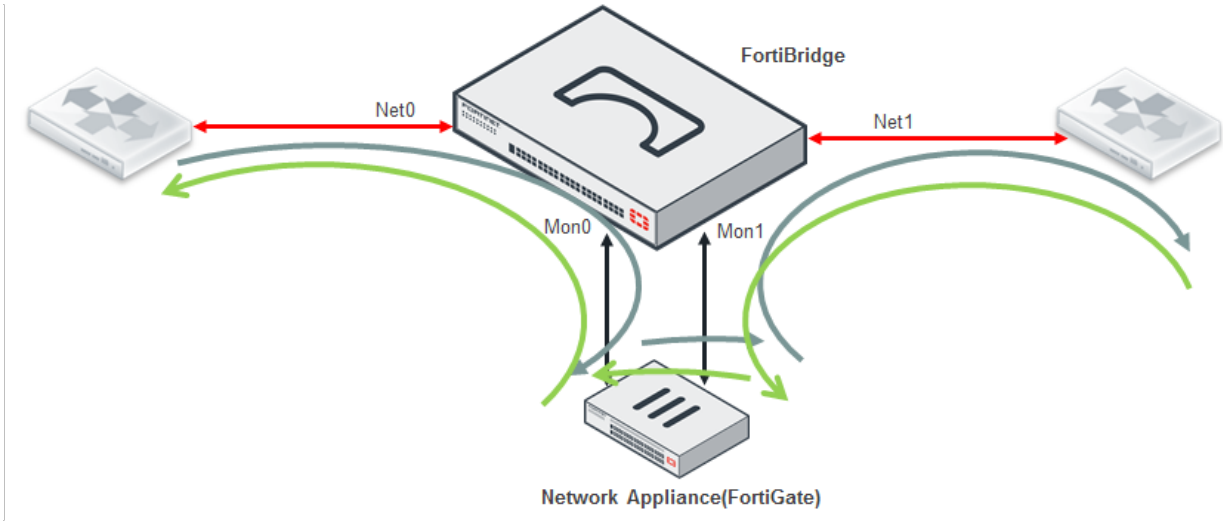
The network ports have built-in transceivers. The monitor ports require plug-in optical transceivers. The correct transceivers are delivered (pre-installed) with your FortiBridge product.

Example FortiBridge Application

You can add a FortiGate unit between your internal network and the Internet. The FortiGate protects the internal network by providing security services (such as virus scanning and web filtering) for all traffic passing to and from the Internet.

If you also add a FortiBridge to the configuration, the internal network will remain connected to the Internet even if the FortiGate unit stops functioning. The FortiBridge will direct the network traffic around the FortiGate unit if a failure occurs.

A FortiBridge segment operates in Inline mode when the FortiGate unit is processing traffic normally. Traffic between the internal network and the Internet flows between the FortiBridge NET0 and NET1 ports. FortiBridge directs the traffic between MON0 and MON1, through the FortiGate unit (see figure below).



In inline mode, the FortiBridge operates at least one probe between the monitor ports, to ensure that network connectivity is maintained. Currently, the FortiBridge supports heartbeat, ping (ICMP) and HTTP probes.

If the probe fails (receiving port fails to receive the probe message within the timeout period), FortiBridge assumes that the FortiGate has failed. FortiBridge transitions into bypass mode and provides notifications by syslog, SNMP, and/or email (these choices are configurable). When the probe has been re-established, the FortiBridge transitions back to inline mode. The exact failure and recovery actions are configurable.

Probe packets must be accepted and passed through the FortiGate. You may need to add firewall policies to the FortiGate unit to ensure that probe packets are not blocked.

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, ping or HTTP 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 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 probes 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

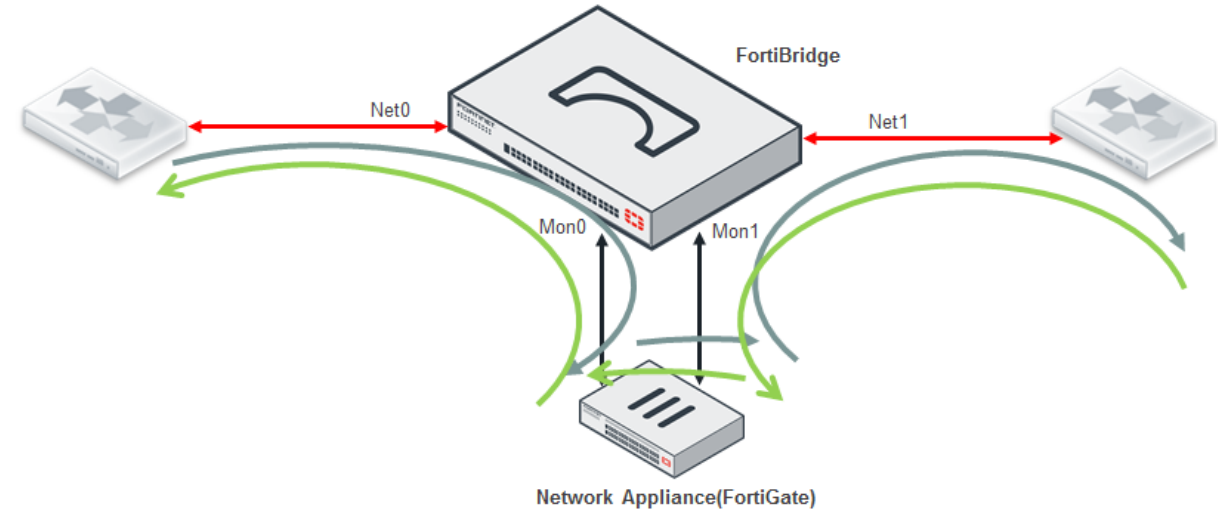
Description

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 traffic 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/Ping/HTTP Probe Failure
- Link Failure
- System Power Failure

The following sections provide details about these mechanisms and their associated recovery actions.

Heartbeat/Ping/HTTP Probes

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

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

If the probe timer expires before a packet is detected, the segment transitions to one of the bypass modes (Bypass, TAP or Fail-cutoff), depending on the configured value of the probe failure action.

By default, the network segment will automatically recover from the probe failure mode back to inline mode when it detects that the failed probe has recovered.

Monitor or Network Link Failure

FortiBridge provides link failure detection for the monitoring ports and the network ports.

If a monitor link fails, the segment may stay in Inline mode or transition to one of the bypass modes (Bypass, TAP or Fail-cutoff), depending on the configured value of the monitor link error mode. If a probe is active on the link, the probe will also fail.

By default, the segment will automatically recover to inline mode from monitor link failure when it detects that the failed probe has recovered.

If a network link fails, the segment may stay in Inline mode or transition to Fail-cutoff mode, depending on the configured value of the network link error mode.The segment requires manual recovery from Fail-cutoff mode.

System Power Failure

If the FortiBridge experiences a power loss, each network segment transitions to passive bypass mode. When power is restored, each segment can auto-recover to inline mode or remain in bypass mode, based on configuration settings.

Probes and FortiGate Policies

Probe packets must be accepted and passed through the FortiGate. You may need to add firewall policies to the FortiGate unit to ensure that probe packets are not blocked. For a configuration example, see section **Configure FortiGate for Probe Packets** in CLI Configuration for Inline mode

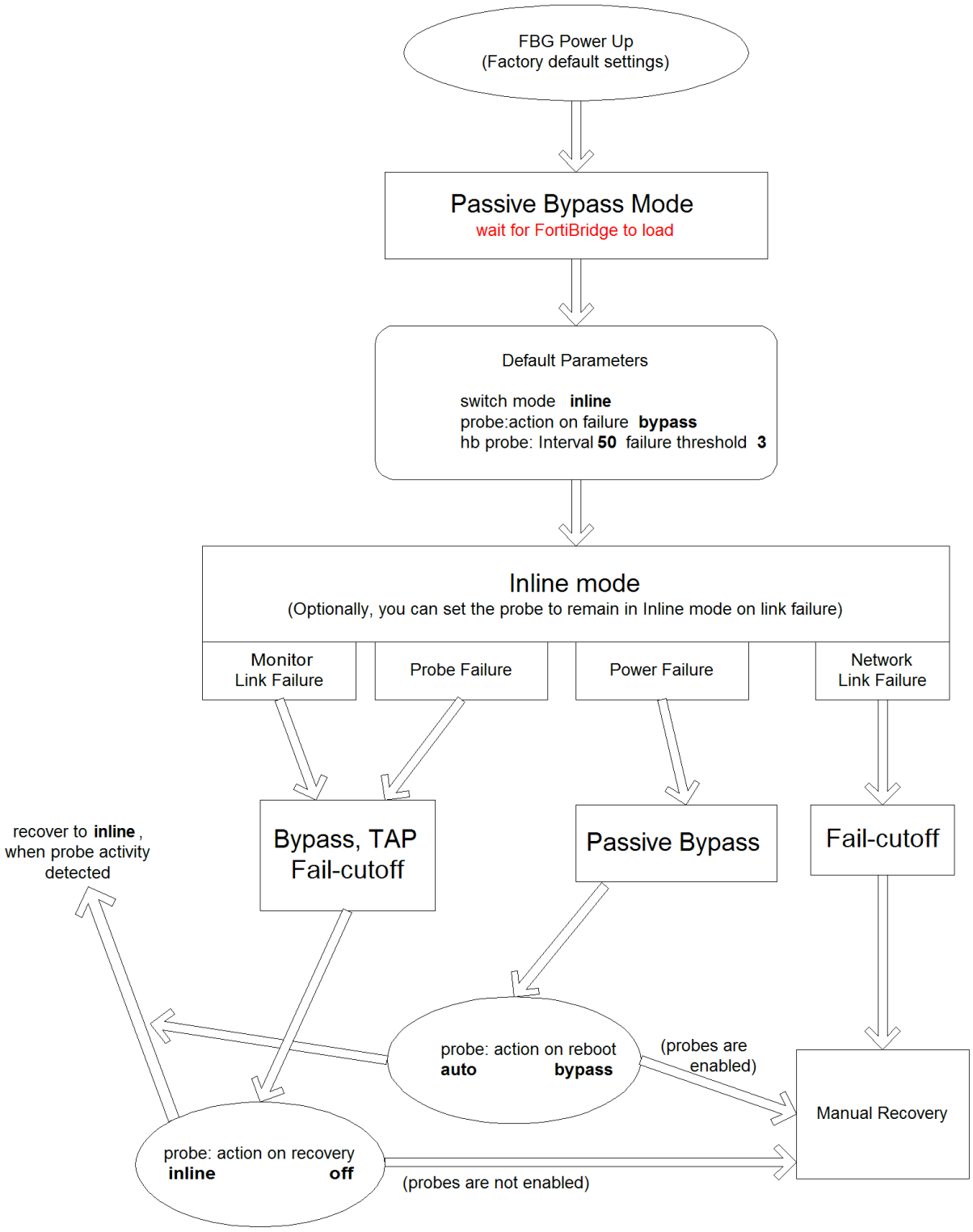
Manual Actions

Using the CLI, you can manually set a segment into Inline, Bypass, TAP or Fail-cutoff mode. You must disable all probes before you can set the mode.

Because there are no probes enabled, the segment will not recover automatically after an error.

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
switch mode inline
probe:action on failure bypass
hb probe: Interval 50 failure threshold 3
Inline mode
(Optionally, you can set the probe to remain in Inline mode on link failure)
Monitor Link Failure
Probe Failure
Power Failure
Network Link Failure
Bypass, TAP Fail-cutoff
Passive Bypass
Fail-cutoff
recover to inline, when probe activity detected
probe: action on reboot
auto bypass
(probes are enabled)
Manual Recovery
probe: action on recovery
inline off
(probes are not enabled)

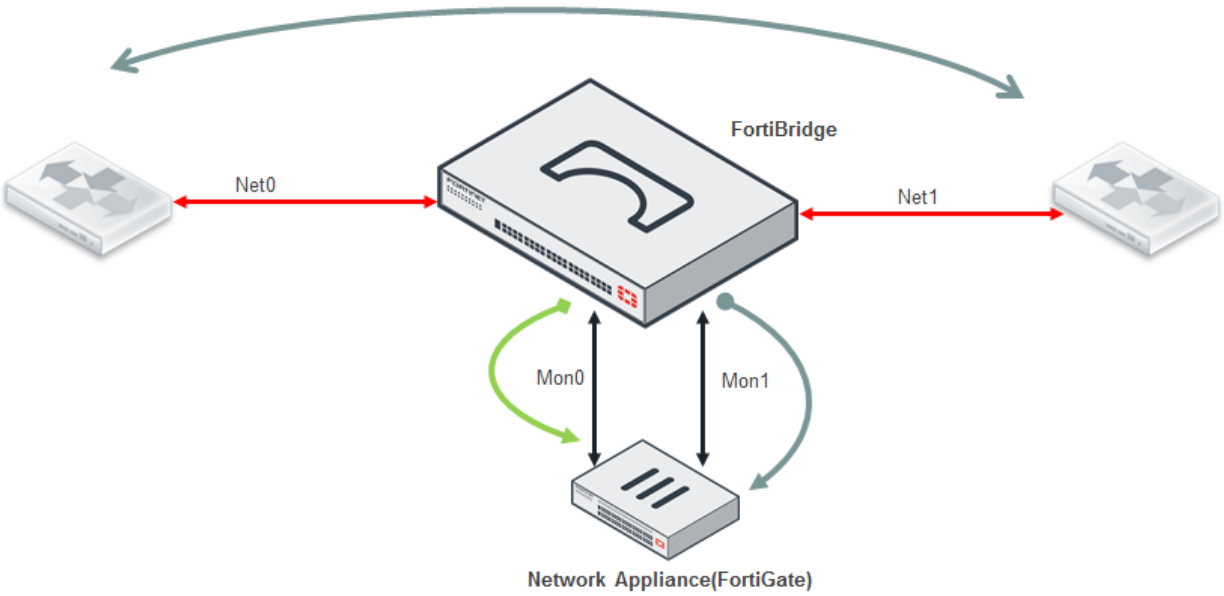
TAP Mode

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).

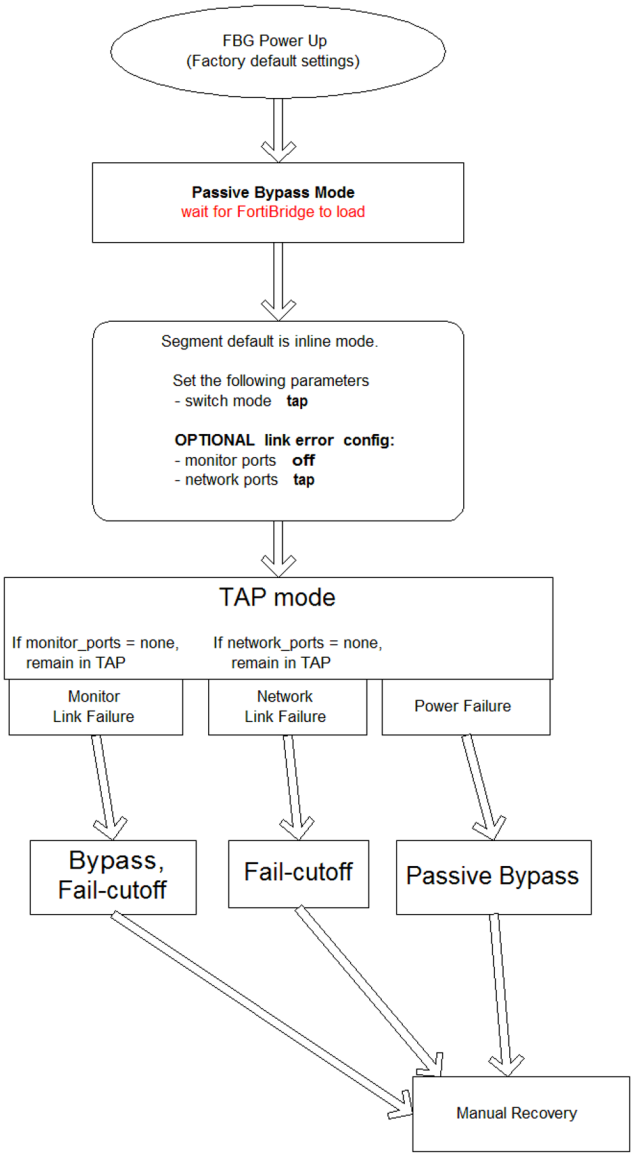
The following diagram shows the packet flow for TAP mode. Traffic flows in both directions between Net0 and Net1. In addition, traffic from Net0 is mirrored to Mon0 and traffic from Net1 is mirrored to Mon1:



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.



Failure Detection and Recovery

The FortiBridge does not provide probes 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:

- Link Failure
- System Power Failure

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

Monitor or Network Link Failure

FortiBridge provides link failure detection for the monitoring ports and the network ports.

For network link or monitor link failures, you can configure the threshold value and whether to raise SNMP traps. For monitor link failure, you can configure the segment to remain in TAP mode or transition to Bypass or Fail-cutoff mode. For network link failure, you can remain in TAP mode or transition to Fail-cutoff mode.

Manual recovery is required. Therefore, for most configurations, we recommend remaining in TAP mode.

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 at the following location:

http://docs.fortinet.com/d/fortibridge-3000x-quickstart

For additional 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.

Create an Access Profile

The admin user is assigned to a predefined access profile. You can create additional access profiles to control user access to the FortiBridge features.

To create an access profile with read-only access:

```
FBG-3002L#config system accprofile
FBG-3002L#edit roprof
FBG-3002L#set admingrp r
FBG-3002L#set loggrp r
FBG-3002L#set sysgrp r
FBG-3002L#set sysshutdowngrp r
```

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 create a new admin user and password:

```
FBG-3002L#config system admin
FBG-3002L#edit myadmin
FBG-3002L#set accprofile admin
FBG-3002L#set password xxxx
```

To create a restricted user:

```
FBG-3002L#config system admin
FBG-3002L#edit FBGuser1
FBG-3002L#set accprofile roprof
```

```
FBG-3002L#set password xxxx
```

You must log out and then log in again to access the new user account.

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#execute date 02 21 2015
FBG-3002L#execute time 10 20
```

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

```
FBG-3002L#config system global
FBG-3002L#set ntpsync enable
FBG-3002L#set ntpserver 192.168.2.100
```

Administrative port settings

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

```
FBG-3002L#config system manageip
FBG-3002L#set ip 192.168.2.200 255.255.0.0
```

You can change the default gateway using the following commands:

```
FBG-3002L#config system route
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#config system global
FBG-3002L#set hostname FBG-3002S
```

Security Settings

TACACS+ and RADIUS authentication

FortiBridge supports TACACS+ and RADIUS authentication for all of the remote access methods (Web Administrative GUI, SNMP access, SSH and Telnet). Supported TACACS+ capabilities include:

- clear and encrypted mode
- Authentication and Accounting

- Inbound Password Authentication Protocol (PAP) login

Use the following commands to enable TACACS+ authentication:

```
FBG-3002L#config system user authentication
FBG-3002L#set auth-type tacacs+
FBG-3002L#set server_ip 192.168.3.2
FBG-3002L#set secret default_key
```

Use the following commands to enable RADIUS authentication:

```
config system user authentication
set auth-type radius
set radius-auth-port 1812
set radius-account-port 1813
```

See the FortiBridge CLI Reference for additional TACACS+/RADIUS commands:

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

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#execute factoryreset
```

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

Firmware Upgrade from the GUI

The FortiBridge GUI supports upgrade procedures starting with release 4.1.0. Use the following GUI steps:

1. Go to **System > Status**.
2. On the **System Information** widget, next to the **Firmware Version** field, click **Update**
3. The web browser will open a pop-up window for you to select the image file.
4. Click **OK** to start the upgrade.
5. The system displays the upgrade progress in the text field of the pop-up window. When the upgrade is complete, the system displays a message indicating the success of the upgrade.
6. On the **Unit Operation** widget, click the **reboot** button.
7. After the restart, log in and verify the firmware version on the **System Information** widget.

Firmware Upgrade from the CLI

Upgrade From 4.0

Upgrading from release 4.0 to 4.1 or later release requires a special procedure. Refer to Troubleshooting for this procedure.

Upgrade From 4.1

To upgrade from release 4.1.0 (or any later release), use the following steps:

1. Copy the new firmware file to the /tftpboot directory of the TFTP server, or to a directory on the SCP server.
2. For a TFTP server, enter the following CLI command:
   ```
   execute restore image tftp <image_file_name> <tftp-server_ipv4> [force]
   ```
3. For an SCP server, enter the following CLI command:
   ```
   execute restore image scp <image_file_name> <remote_path> <ssh-server_ipv4>
   <username> [force]
   ```
4. When the upgrade is complete, enter the following CLI command:
   ```
   reboot
   ```

Configuration using GUI Interface

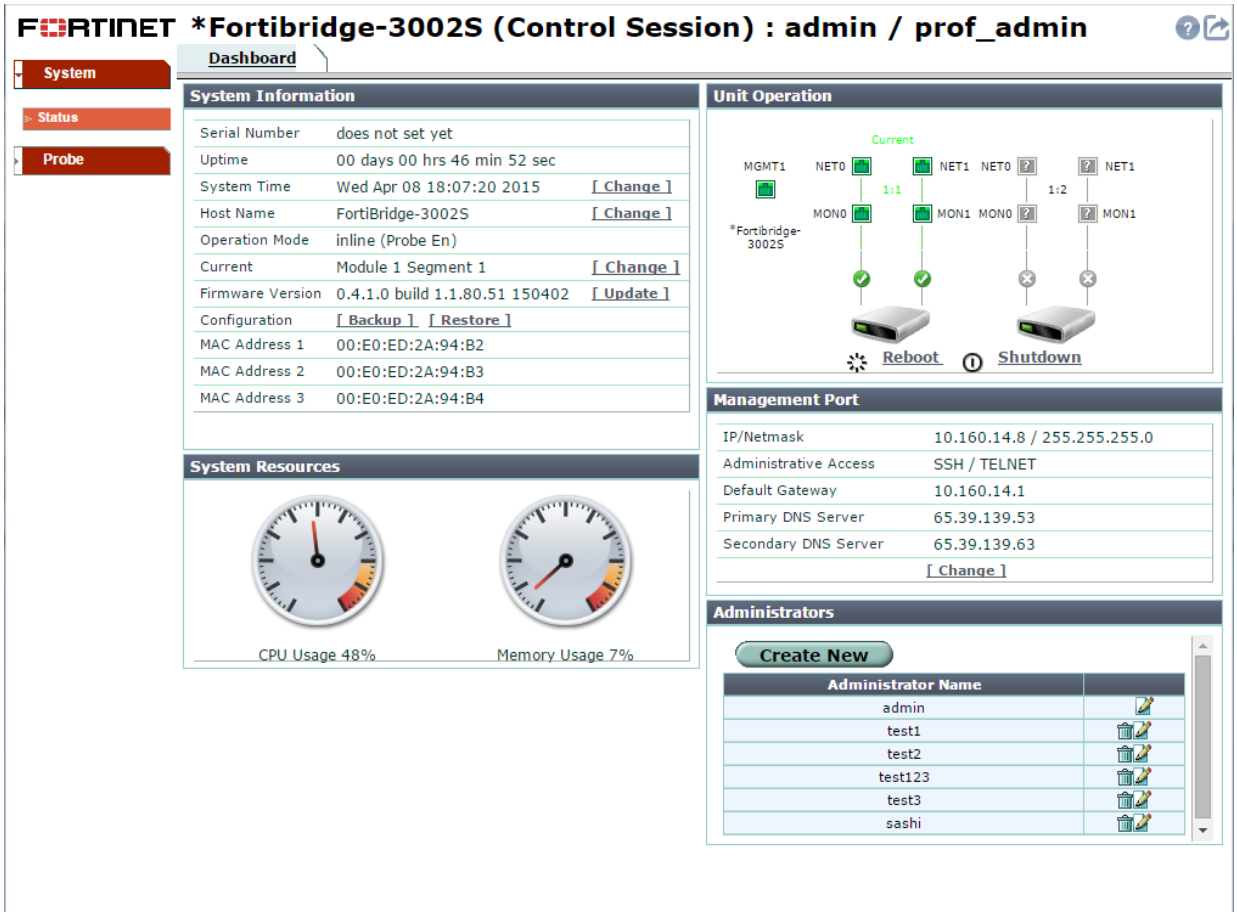
The Administrative GUI Interface is a browser-based tool for configuring and managing the FortiBridge product.

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:



Settings Summary

The following sections provide a summary of how to configure a segment into Inline, Bypass, or TAP mode.

Settings for Inline mode:

- check **Preserve on reboot** if you want the probes to remain enabled after a reboot.
- enable at least one probe

Settings for Bypass mode:

- disable all of the probes
- set **Operation Mode** (in System Information) to Bypass

Settings for TAP mode:

- disable all of the probes
- set **Operation Mode** (in System Information) to TAP

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. Click **Change** to adjust the date or time. If NTP synchronization is enabled, NTP will override any manual changes.
Host Name	The host name appears at the CLI prompt and as the SNMP system name. Click **Change** to edit the system name.
Operation Mode	Displays the mode for the current segment. By default, the segment automatically transitions to the Inline mode. You can only change the operation mode after you disable all probes on this segment.
Current	The chassis supports up to three modules. If this system is provisioned with more than one module, you can click **Change** to edit the value of the current module. If the current module supports more than one segment, you can also edit the value of current segment.
Firmware version	Current firmware version. To perform an upgrade, click **Update**. 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. This is a read-only field.
MAC Address 2	MAC address of the MON0 port (for the current segment). This is a read-only field.
MAC Address 3	MAC address of the MON1 port (for the current segment). This is a read-only field.

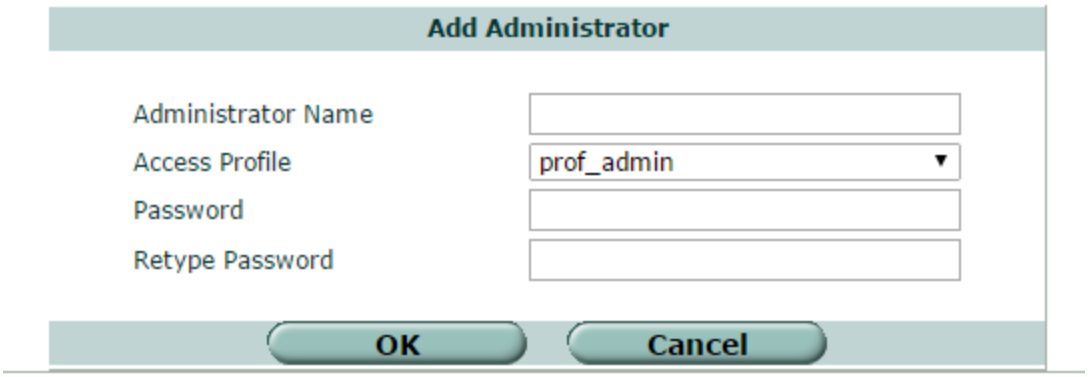
Management Port

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

IP/Network	The IP address and mask of the management port.
Administrative Access	Check boxes to enable SSH and/or Telnet access.
Default Gateway	The default gateway for the management port.
Primary DNS Server	IP address of the primary DNS server.
Secondary DNS Server	IP address of the secondary DNS server.

Administrators

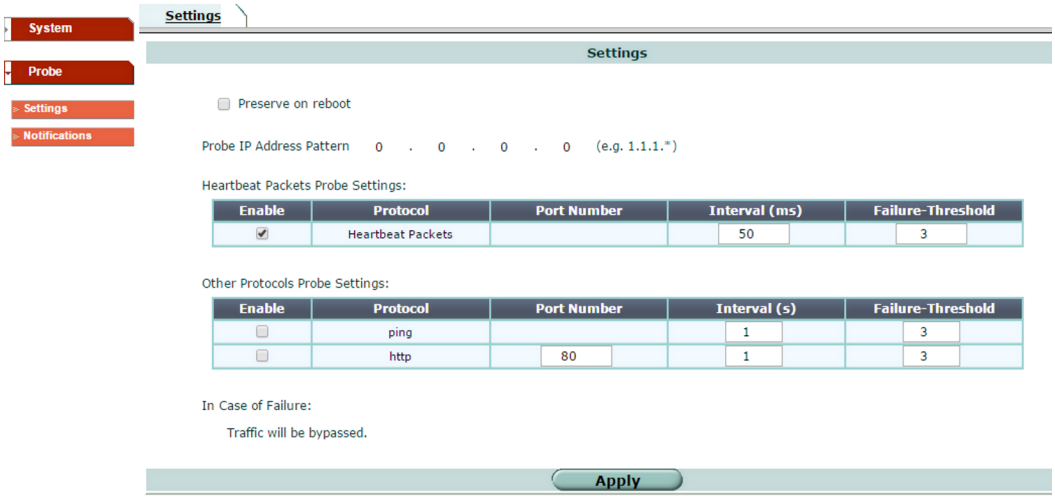
Click on the edit button to change the administrator user name or password. The system opens a pop-up window with the following fields:



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.

Note: You must enable at least one probe for the segment to transition automatically to Inline mode. If no probe is enabled, the segment will remain in Bypass mode (unless you change the Operation Mode manually).

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

Preserve on reboot	If you check this option, the system will preserve the active probes across a reboot.
Probe IP Address Pattern	Defines the range of IP addresses that active probes will use. Click on each digit to edit the value. When you click Apply, active probes immediately start to use the new IP addresses.

There are 2 additional probe settings that you can change only through the CLI:
action_on_recovery - default action is to recover to inline mode
action_on_reboot - default action is to auto-recover to inline mode.

For additional information, refer to CLI Configuration for Inline mode

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 segment transitions to the configured probe-failure mode (the default is bypass mode).

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

Other Protocol Probe Settings

You can enable an HTTP probe and/or a ping probe. Configure the following settings:

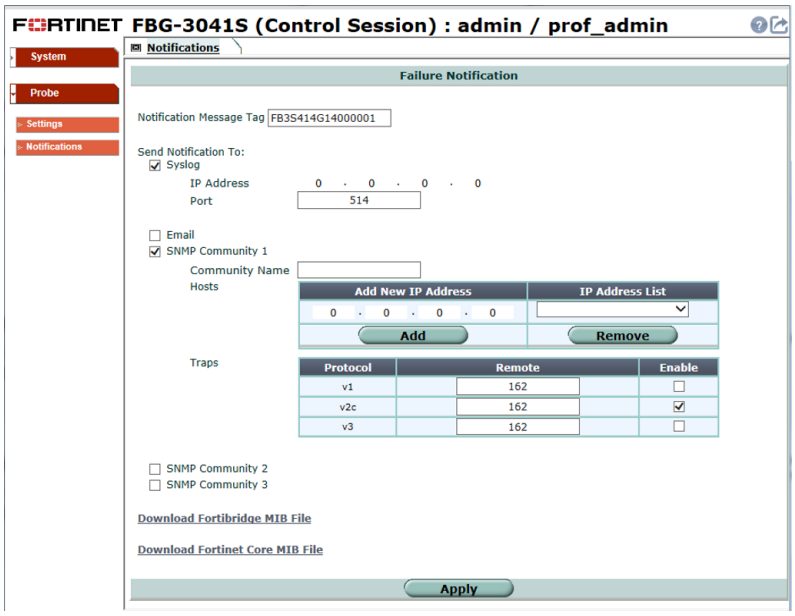
Enable	Enables the probe.
Port Number	(HTTP probe) Destination port number in the HTTP message.
Interval	The interval (in seconds) that the system will wait before sending the next probe message.
Failure Threshold	The failure threshold defines the maximum time (in seconds) that the receiving port will wait for the next message. If the message is not received within this time, the segment transitions to the configured probe-failure mode (the default is bypass mode).

Notifications

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

This page also includes links to download the FortiBridge MIB file and the Fortinet core MIB file.

The following figure shows the notifications page:



The FortiBridge supports the following notification types:

- Syslog
- Email
- SNMP

For **Syslog**, the probe notification fields are described in the following table:

Notification Message Tag	Text tag that the system will add to Syslog entries.
Syslog	Select this option to enable Syslog notifications.
IP Address	IP address of the syslog device.
Port	Destination port for the syslog messages.

For **email**, no additional probe notification fields are required. You must configure the system-wide email notification fields using the CLI (see "AlertEmail Commands" in the FortiBridge 4.1.0 CLI Reference).

For **SNMP**, you can configure probe notifications for up to three SNMP communities.

If you enter text in the Notification Message Tag Text, the system will add this text to all SNMP trap entries.

For each SNMP Community, the notification fields are described in the following table:

Community Name	The SNMP community name.
Hosts	Add IP addresses of up to 8 SNMP managers.
Traps	Enable the desired SNMP version. Configure the remote port number.

CLI Configuration for Inline mode

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

With the default configuration values, the system automatically transitions each network segment into Inline mode.

To restore a segment to inline operation, set the following values:

- Set the current module and segment
- Set switch mode to be inline
- Configure probe settings:
  - action_on_failure: bypass
  - action_on_recovery: inline
  - action_on_reboot : auto
  - preserve_on_reboot : disable
- Configure the heartbeat probe:
  - status: enable
  - probe interval: 50
  - failure-threshold: 3
- (Optional) Set the link error threshold and actions
- (Optional) Define a custom heartbeat packet

The following sections provide information about these parameters.

Set Current Module and Segment

For the **set segment** command, enter the module number and segment number separated by a space:

```
FBG-3002L#config system global
FBG-3002L#set segment 1 2
```

Set Switch Mode

By default,the segment is automatically set to inline mode. You can also manually set the switch mode for the current segment to **inline**:

```
FBG-3002L#execute switch_mode inline
```

Configure Probe Settings

Enter the following command to configure the probe settings:

```
FBG-3002L#config probe setting
```

action_on_failure

Use the following command to set the probe failure mode (bypass, failcutoff, or tap) for the current segment. The default value is **bypass**. The system will transition this segment to the failure mode if probe failure is detected.

```
set action_on_failure failcutoff
```

action_on_recovery

When a segment is ready to recover from probe failure (probe packets are now detected), by default the segment will recover to Inline mode. If you set action_on_recovery to off, the segment will remain in the action_on_failure mode:

```
set action_on_recovery off
```

action_on_reboot

After a reboot, the segment will automatically recover to Inline mode. If you set action_on_reboot to bypass, the segment will remain in bypass mode after a reboot.

```
set action_on_reboot bypass
```

preserve_on_reboot

After a reboot, the segment will automatically enable all configured probes, even probes that were in a disabled state prior to the reboot. If you enable **preserve_on_reboot**, the segment will enable only the probes that were in an enabled state prior to the reboot.

```
set preserve_on_reboot enable
```

Configure the Heartbeat Probe

Enable the heartbeat probe for the current segment:

```
FBG-3002L#config probe probe_list heartbeat
FBG-3002L#set status enable
```

Use the following 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 probe failure action.

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

```
FBG-3002L#set probe_interval 10
FBG-3002L#set failure_threshold 40
```

By default, the heartbeat is sent by Mon0 and received at Mon1. You can reverse the direction of the heartbeat:

```
FBG-3002L#set send_on_port MON1
```

You can also set the probe to be bidirectional, as shown in the following example:

```
FBG-3002L#set send_on_port bidirectional
FBG-3002L#set failure_criteria bidirectional
```

Set Link Error Mode

Use the **config probe setting rx_tx_error_mode** command to set the actions for monitor link failure and network link failure.

The following table describes the sub-commands and their parameters:

trap {enable | disable}	enable or disable. Enables the sending of SNMP traps if a link fails.
timeout <timeout>	Integer greater than 0. The minimum interval (in seconds) between SNMP traps.
monitor_ports {none| bypass | tap | failcutoff}	Configure the mode that the segment will transition into in the event of a monitor port error.
network_ports {none | failcutoff}	Configure the mode that the segment will transition into in the event of a network port error.
threshold <threshold>	Integer greater than 0. Specifies the maximum allowable number of errors per second on a link before the link is . The default value is 10.

In the following example configuration, traps are enabled, with a maximum of one trap per minute. The segment will send SNMP traps if either network link exceeds 20 errors per second. The segment transitions to Bypass mode if a monitor port fails, and to Fail-cutoff if a network port fails.

```
FBG-3002L#config probe setting rx_tx_error_mode
FBG-3002L#set trap enable
FBG-3002L#set timeout 60
FBG-3002L#set monitor_ports bypass
FBG-3002L#set network_ports failcutoff
FBG-3002L#set threshold 20
```

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#execute hb_packet load <tftp server IP address>
```

Restore the Heartbeat contents to the default content:

```
FBG-3002L#execute hb_packet default
```

To view the Heartbeat contents:

```
FBG-3002L#execute hb_packet display
```

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

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

Configure FortiGate for Probe Packets

The FortiBridge probes rely on the inline network device to pass the probe 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 probe packets.

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. The FortiBridge probes are configured to use IP addresses 2.3.4.*, so mon0 and mon1 are in the same subnet:

Define mon0 and mon1:

```
config firewall address
   edit "mon0"
      set associated-interface "port10"
      set subnet 2.3.4.0 255.255.255.0
   next
   edit "mon1"
      set associated-interface "port11"
      set subnet 2.3.4.0 255.255.255.0
   next
end
```

Define firewall policy for the PING probe:

```
config firewall policy
   edit 1
      set srcintf "port10"
      set dstintf "port11"
      set srcaddr "mon0"
      set dstaddr "mon1"
      set action accept
      set schedule "always"
      set service "ALL_ICMP"
      set logtraffic all
      set capture-packet enable
      set auto-asic-offload disable
   next


   edit 2
      set srcintf "port11"
      set dstintf "port10"
```

```
      set srcaddr "mon1"
      set dstaddr "mon0"
      set action accept
      set schedule "always"
      set service "ALL_ICMP"
      set logtraffic all
      set capture-packet enable
      set auto-asic-offload disable
   next
end
```

Define firewall policy for the HTTP probe:

```
config firewall policy
   edit 1
      set srcintf "port10"
      set dstintf "port11"
      set srcaddr "mon0"
      set dstaddr "mon1"
      set action accept
      set schedule "always"
      set service "HTTP"
      set logtraffic all
      set capture-packet enable
      set auto-asic-offload disable
   next


   edit 2
      set srcintf "port11"
      set dstintf "port10"
      set srcaddr "mon1"
      set dstaddr "mon0"
      set action accept
      set schedule "always"
      set service "HTTP"
      set logtraffic all
      set capture-packet enable
      set auto-asic-offload disable
   next
end
```

Define firewall policy for other traffic:

```
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"
      set logtraffic 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"
       set logtraffic all
    next
end
```

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
- disable all probes
- switch mode: set to TAP
- (Optional) Set the link error threshold and actions

Set Current Module and Segment

For the **set segment** command, enter the module number and segment number separated by a space:

```
FBG-3002L#config system global
FBG-3002L#set segment 1 2
```

Disable Probes

Disable all probes for the segment.

```
FBG-3002L#config probe probe-list heartbeat
FBG-3002L#set status disable
FBG-3002L#config probe probe-list ping
FBG-3002L#set status disable
FBG-3002L#config probe probe-list http
FBG-3002L#set status disable
```

Set Switch Mode to TAP

Once the probes are disabled, you can set the segment to TAP mode:

```
FBG-3002L#execute switch-mode tap
```

Set Link Error Mode

Use the set rx_tx_error_mode command to set the actions for monitor link failure and network link failure.

The following table describes the sub-commands and their parameters:

trap {enable | disable}	enable or disable. Enables or disables traps.
timeout <timeout>	Integer greater than 0. The minimum interval (in seconds) between traps.
monitor_ports {none| bypass | tap | failcutoff}	Configure this value as **tap**, to keep the segment in TAP mode.
network_ports {none | failcutoff}	Configure this value as **tap**, to keep the segment in TAP mode.
threshold <threshold>	Integer greater than 0. Specifies the maximum allowable number of errors per second on a link. The default value is 10.

In the following example configuration, traps are enabled, with a maximum of one trap per minute. The segment will send SNMP traps if either network link exceeds 20 errors per second. The segment remains in TAP mode.

```
FBG-3002L#config probe setting rx_tx_error_mode
FBG-3002L#set trap enable
FBG-3002L#set timeout 10
FBG-3002L#set monitor_ports tap
FBG-3002L#set network_ports tap
FBG-3002L#set threshold 20
```

NOTE: The system does not perform auto-recovery to Tap mode. When the error has cleared, you need to manually restore the segment. Therefore, we recommend that you configure the **network_port** and **monitor_port** values as **tap**, so that the segment remains in TAP mode in the event of link errors.

CLI Configuration for Bypass Mode

This section describes the configuration tasks required for a network segment to operate in Bypass 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 Bypass mode:

- Set the current module and segment
- disable all probes
- switch mode: set to **bypass**

Set Current Module and Segment

For the **set segment** command, enter the module number and segment number separated by a space:

```
FBG-3002L#config system global
FBG-3002L#set segment 1 2
```

Disable Probes

Disable all probes for the segment.

```
FBG-3002L#config probe probe-list heartbeat
FBG-3002L#set status disable
FBG-3002L#config probe probe-list ping
FBG-3002L#set status disable
FBG-3002L#config probe probe-list http
FBG-3002L#set status disable
```

Set Switch Mode to Bypass

Once the probes are disabled, you can set the segment to Bypass mode:

```
FBG-3002L#execute switch-mode bypass
```

CLI Configuration for Modules

The FortiBridge host system houses up to three bypass modules.

A bypass module supports one or more network segments. Each network segment supports one Inline/TAP/Bypass configuration. 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".

Select the Current Module

Set the module and segment to be current:

```
FBG-3002L#config system global
FBG-3002L#set segment 1 1
```

Enter the following command to display the current module and segment :

```
FBG-3002L#get segment
```

Enter the following command to blink the Status OK LED on the current module:

```
FBG-3002L#execute show-module enable
```

List the Module Properties

Displays the settings for each of the installed modules.

```
FBG-3002L#get hardware status
```

Display the Module State

Displays information about the state of the current module.

```
FBG-3002L#get system status
```

Set the Link Speed

The 10G bypass modules support dual-rate link speed (1G or 10G). To set the link speed, use the set interface_ 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#config system global
FBG-3002L#set interface_speed [all] (auto | 10g | 1g)
```

Optional Segment Features

Two Port Link

Use the following commands to enable the Two Port Link feature. With this feature enabled, if one of the network links fails, the system will drop the link on the other network port.

```
FBG-3002L#config system fail_close
FBG-3002L#set network_to_network enable
```

Monitor-Network Port Link

Use the following commands to enable the Monitor-Network Port Link feature. With this feature enabled, if one of the monitor links fails, the system will drop the link on the network port. You can also specify which monitor link will trigger the feature (the default is mon0).

```
FBG-3002L#config system fail_close
FBG-3002L#set set monitor_to_network enable
FBG-3002L#set set monitor_to_network ports {all | mon0 | mon1}
```

Troubleshooting

CLI Command Syntax

The CLI commands in the FortiBridge 4.0 release are documented in the CLI-Reference-Version-4.0.

In the FortiBridge 4.1 release, the CLI commands were changed to align with standard Fortinet CLI command syntax. These commands are documented in the CLI Reference-Version-4.1.

In the FortiBridge 4.1 or later release, you can use the following commands to convert the FortiBridge CLI to use the 4.0 command set:

```
diagnose debug application
sil_cmd enable
```

Use the following commands to convert the FortiBridge CLI to the 4.1 CLI command set:

```
fort_cli enable
```

If the command is unknown, the CLI is already set for the 4.1 command set.

Firmware Upgrade From 4.0

Starting in release 4.1.0, FortiBridge supports a different format for image files compared to 4.0. Therefore, upgrade from 4.0 requires two steps:

A. upgrade to the new file format.
B. upgrade to the latest 4.1 build.

A. Upgrade to the new file format

1. Copy the old-format firmware files and the matching 'update.desc' file to the /tftpboot directory of the TFTP server. These files are available to Fortinet support staff only, at the following location: http://172.30.71.240/images/misc/Old_file_format/
2. Enter the following CLI command:
   `update <tftp server IP address>`
3. When the upgrade is complete, you need to power-cycle the chassis.
   1. Enter the shutdown command: `execute shutdown`
   2. When the shutdown is completed, power on the unit.

B. Upgrade to the latest 4.1 build.

1. Verify that the CLI syntax is set for the 4.1 command set. (See the **CLI Command Syntax** section above)
2. Copy the latest release 4.1 firmware file to the /tftpboot directory of the TFTP server.
3. Enter the following CLI command:
   `execute restore image tftp <image_file_name> <tftp-server_ipv4>`

4. When the upgrade is complete, enter the following CLI command:
   ```
   reboot
   ```