White Paper

# BIG-IP ASM plus iBypass Switch

## iBypass Switch maximizes application uptime.

by F5 Networks and Net Optics

# Contents

**Introduction** **3**

**How it works** **4**

Bypass Off 4

Bypass On 4

Heartbeat™ Packet 5

**iBypass™ Switch** **6**

Media conversion 6

Remote management 7

Integrated traffic monitoring 8

Heartbeat packet options 10

Configuring the ports 12

Taking BIG-IP ASM Offline 13

**Summary** **14**

# Introduction

BIG-IP Application Security Manager (ASM) is an in-line Web application firewall appliance that protects enterprise applications from targetted security threats which can seriously impact corporations. But any time a device is deployed in-line, it introduces a potential point of failure in the network, because it can stop traffic dead in its tracks if the device loses power or experiences some types of failures.

To minimize the risk of network down time, many organizations deploy in-line appliances with companion Bypass Switches, which are devices specifically designed to keep network traffic flowing in the event of a power or appliance failure. One such device is the Net Optics 1 GigaBit iBypass™ Switch, which creates a fail-safe, fail-to-wire access port for an in-line device. It also provides additional value-add with integrated traffic instrumentation and remote management capability.

The operation of a Bypass Switch with BIG-IP ASM is discussed in the following section. After that, the features and options of the Net Optics 1 GigaBit iBypass Switch are explained.

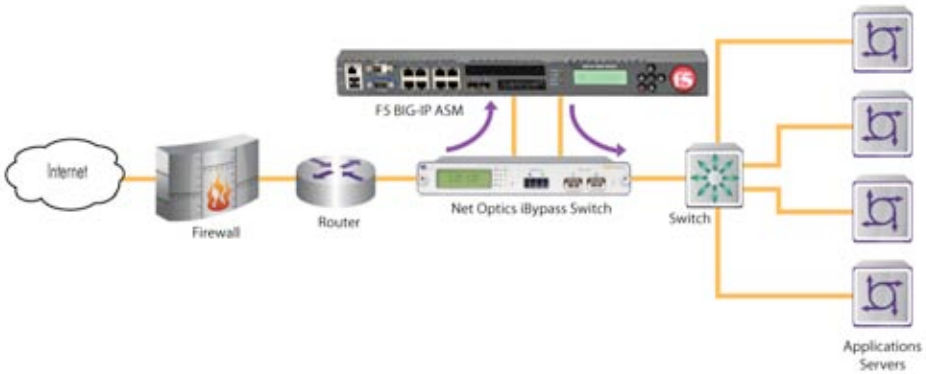


**Figure 1: BIG-IP ASM deployed with an external Bypass Switch**

# How it works

BIG-IP ASM needs in-line access to all of the network traffic so it can detect security threats and prevent them from entering the network. While BIG-IP ASM is designed and manufactured to the highest levels of reliability, an extra layer of protection to ensure availability of business-critical applications can be obtained by deploying the appliance in conjunction with an external Bypass Switch device. The Bypass Switch keeps network traffic flowing when power fails to BIG-IP ASM or to the Bypass Switch itself. It also opens the link to traffic flow if BIG-IP ASM becomes unavailable for any reason, and the Switch can be commanded through a remote management interface to take BIG-IP ASM offline whenever desired. Let's take a look at how a Bypass Switch accomplishes these operations.

## Bypass Off

The Bypass Switch operates in two modes, Bypass Off and Bypass On. In Bypass Off mode, traffic is routed through BIG-IP ASM exactly as if BIG-IP ASM were in-line itself.

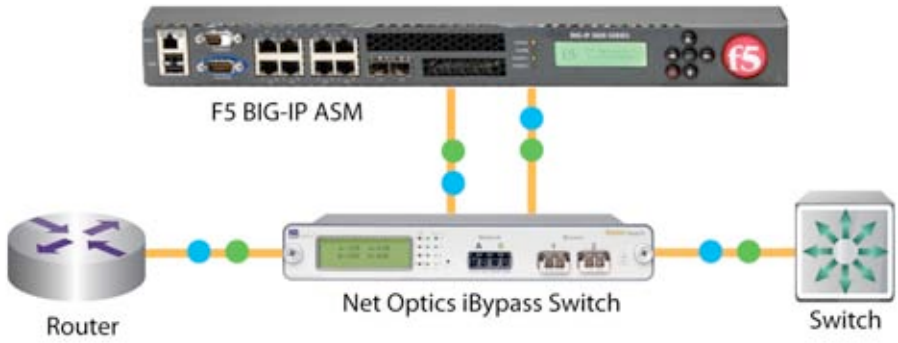


**Figure 2: In Bypass Off mode, all traffic passes through BIG-IP ASM**

## Bypass On

If power is removed from the Bypass Switch, it automatically switches to Bypass On mode. In this mode, traffic passes straight through the Bypass Switch, bypassing BIG-IP ASM.

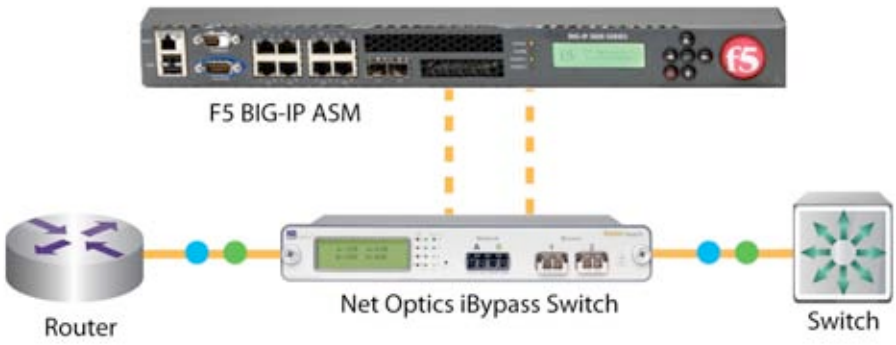


**Figure 3: In Bypass On mode, traffic bypasses BIG-IP ASM**

Bypass On mode is implemented by incorporating optical switches (for fiber media) or relays (for copper media) in the Bypass Switch. The optical switches or relays have a passive (power off) state that enables traffic to flow on the link when the unit has no power.

## Heartbeat™ Packet

If the same power sources (BIG-IP ASM and most Bypass Switches have dual redundant power supplies) supply both BIG-IP ASM and the Bypass Switch, then the optical switches or relays keep traffic flowing in a power fail condition. But what if power fails to BIG-IP ASM but not to the Bypass Switch? Or what if BIG-IP ASM is unable to pass traffic for some other reason, such as a cable being unplugged?

In order to protect against any and all conditions that may make BIG-IP ASM unavailable to process traffic, the Bypass Switch continuously monitors the health of BIG-IP ASM by sending a Heartbeat™ packet through the appliance. The small Heartbeat packet is periodically injected in the traffic stream going to one of BIG-IP ASM's ports, and the Bypass Switch looks for the packet to be returned on the other port. BIG-IP ASM doesn't have to do anything special with the Heartbeat packet; it just passes it like normal traffic. If the Bypass Switch does not see the Heartbeat packet come back within a (programmable) timeout period, and after a (programmable) number of retries, it knows that an error condition exists and so it switches into Bypass On mode, bypassing BIG-IP ASM.

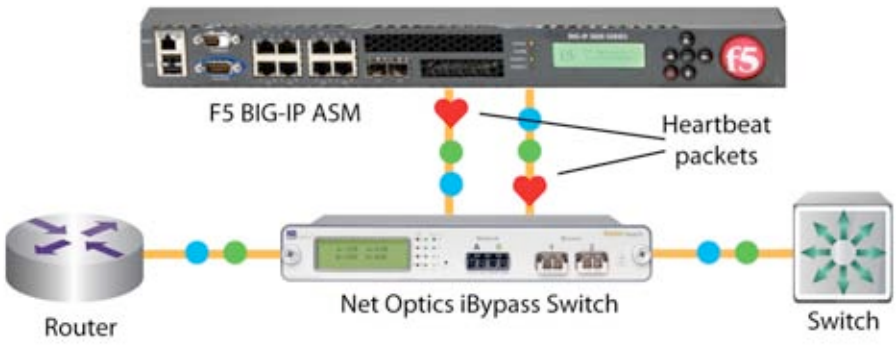


**Figure 4: A Heartbeat packet monitors the health of BIG-IP ASM**

While in Bypass On mode, the Bypass Switch continues to send Heartbeat packets to BIG-IP ASM. As soon as a Heartbeat packet is returned, it knows BIG-IP ASM is healthy again and it switches back to Bypass Off mode, sending the traffic through BIG-IP ASM once again.

# iBypass™ Switch

The Net Optics 1 GigaBit iBypass™ Switch has been tested and qualified with BIG-IP ASM, and shown to provide increased network reliability. Besides the basic Bypass Switch functionality described in the previous section, the iBypass Switch provides value-add features and options including media conversion, remote management, integrated traffic monitoring, and programmable Heartbeat packet parameters.

## Media conversion

Net Optics offers the iBypass Switch in an all-copper model, with 10/100/1000 copper ports for both the network link and the monitor (BIG-IP ASM) ports. Models for SX and LX fiber networks are also available. The fiber models have modular SFP monitor ports, so they support either copper or fiber BIG-IP ASM interfaces. By using copper transceivers in the SFP ports, copper links can be used to connect BIG-IP ASM to the iBypass Switch within a fiber network, saving cost compared to using fiber links. A 10 GigaBit iBypass Switch is also available for higher speed in-line devices.

| iBypass Switches | Part Number | Speed | Network Ports | Monitor Ports |
|---|---|---|---|---|
|  | iBP-HBCU3 | 1 Gigabit | 10/100/1000 Copper | 10/100/1000 Copper |
|  | iBPO-HBSX-SFP<br>iBPO-HBLX-SFP | 1 Gigabit | SX (Multi-mode) Fiber<br>LX (Single-mode) Fiber | SFP (SX, LX, or Copper) |
|  | iBPO-HBSR-XFP<br>iBPO-HBLR-XFP | 10 Gigabit | SR (Multi-mode) Fiber<br>LR (Single-mode) Fiber | XFP (SR or LR) |

**Figure 5: iBypass Switch models from Net Optiocs**

## Remote management

Remote device management saves time and money because it eliminates the need to physically visit the device in order to check its status, reconfigure it, or change its state. In the case of a Bypass Switch, the capability to remotely force it into Bypass On mode is particularly valuable, because it enables operators to take the attached BIG-IP ASM offline at any time – for example, if a new rule set doesn't seem to be performing as expected.

Net Optics Indigo™ device management software provides a variety of tools to remotely manage iBypass Switches. The Indigo software suite, which is included with every iBypass Switch, has a text-based command-line interface (CLI) and a platform (Windows) based tool named System Manager. Indigo also includes the Web-browser-based Web Manager, probably the quickest and easiest tool for new users.

The CLI operates over a local RS232 serial port, while System Manager and Web Manager are accessed through a dedicated management port. The management port can be connected through a switch to an intranet or the Internet, providing remote access to the iBypass Switch from anywhere in the world. Alternately, the management port can be isolated on a protected management VLAN for increased security.

Web Manager is accessed simply by typing the IP address of the iBypass Switch into any browser with a path to the device's management port. A username and password (default: netoptics, netoptics) prevent unauthorized access to the device.


**Figure 6: Indigo™ Web Manager for the iBypass Switch**

## Integrated traffic monitoring

Figure 6 shows the top part of the main Web Manager page. It shows the traffic monitoring capabilities built into the iBypass Switch. The top part of the screen,

labeled Bypass System Status, shows the state of each link as UP or DOWN; Ports A and B are the two network ports, and Ports 1 and 2 are the monitor ports connected to BIG-IP ASM. The link (port) speeds and the status of the two power supplies are also displayed. In the last line of the section, the field Bypass State indicates whether the Switch is currently in Bypass Off (Out) or Bypass On (In) mode. The Check HB (Heartbeat) Packet button is discussed later.

Below the Bypass System Status are four sections that show statistics about the traffic received at each of the ports. For each port, you can easily view these remote monitoring (RMON) statistics:

- **Peak Rate (%)** – The highest bandwidth utilization seen since the last reset
- **Peak Date & Time** – The date and time that the Peak Rate occurred
- **Current Utilization Rate** – The current bandwidth utilization on the port
- **Total Packets** – Count of the number of packets received by the port
- **Total Bytes** – Count of the number of bytes received by the port
- **CRC Errors** – Count of the number of packets received with CRC errors
- **Collision Packets** – Count of the number of packet collisions on the wire
- **Oversize Packets** – Count of the number of packets larger than 1,518 bytes

The iBypass Switch also presents some of the RMON statistics (Current Utilization Rate, Peak Rate, and Peak Date & Time) on its front panel LCD for an at-a-glance view of link and BIG-IP ASM health.

This rich set of traffic information enables significant traffic monitoring and problem solving without the need to attach any separate monitoring tools. In addition, it provides a baseline of information so the right tools can be mobilized when more complex investigations are required.

## Heartbeat packet options

Net Optics designed the iBypass Switch for easy plug-and-play deployment. In most cases, installation consists of simply plugging in the cables and applying power – operation is full automatic. However, it may be useful to customize the Heartbeat packet in some environments. This is easily accomplished using the Indigo Web Manager, System Manager, or CLI tools.

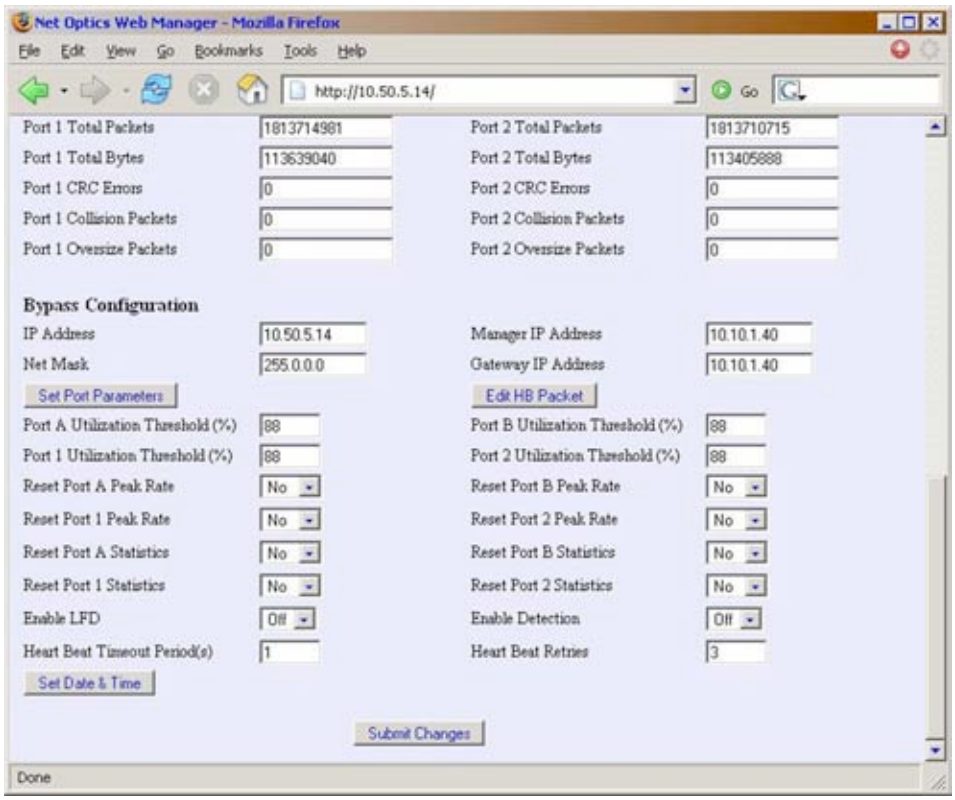


**Figure 7: Web Manager configuration section**

Figure 7 shows the lower part of the main Web Manager page. At the bottom of the screen, below a variety of other configurable parameters (including the flags to clear the port statistics counters and peak rate information), are fields for setting the Heart Beat Timeout Period(s) and the Heart Beat Retries. The Heart Beat Timeout Period(s) is the amount of time, in seconds, that the iBypass Switch waits to see if a Heartbeat packet is returned after it is sent to the BIG-IP ASM appliance.

The default timeout is 1 second, but it can be increased if this isn't enough time, for example if BIG-IP ASM may occasionally introduce a long latency in your environment. The Heart Beat Retries parameter sets the number of times in a row that the Heartbeat packet is not returned before the Switch is triggered to enter Bypass On mode. The default is 3 – the original Heartbeat packet plus two retries.

Setting the Heart Beat Timeout Period(s) to 0 has a special meaning; it is the way to force the iBypass Switch into Bypass On mode. Enter a 0 in this field and click Submit Changes to instantly take BIG-IP ASM offline. The offline condition persists until you set Heart Beat Timeout Period(s) to a non-zero value.

It is also possible to change the Heartbeat packet itself. The default Heartbeat packet works correctly in most environments, but it could be blocked by customized rules in BIG-IP ASM. If this happens, the Heartbeat packet can be changed to something that does not trigger the rule.

The current Heartbeat packet can be viewed by clicking the Check HB Packet button near the top of the main Web Manager screen. (Select Yes to Refresh the Packet list and click Apply to refresh the displayed packet.)

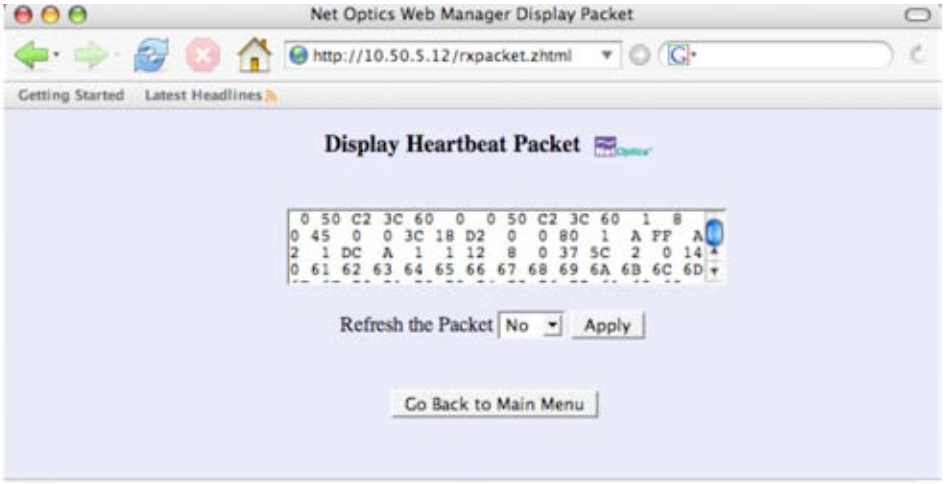


**Figure 8: Web Manager displays the current Heartbeat packet values**

To change the Heartbeat packet contents, click the Edit HB Packet button in the configuration section near the bottom of the screen. Then simply change the hex

values in the form that appears and click Submit the Packet. (Be sure to adhere to IP and MAC address conventions, and generate a correct CRC.)

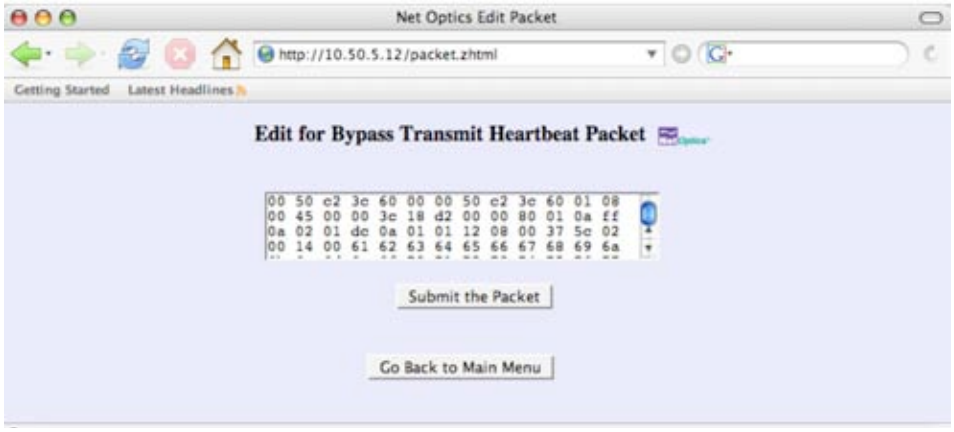


**Figure 9: Web Manager enables the Heartbeat packet content to be changed**

Between configuring the Heart Beat Timeout Period(s) and the Heart Beat Retries, and changing the packet contents as well, you have complete flexibility to tune the Heartbeat packet for your system.

## Configuring the ports

The Indigo tools also allow you to enable and disable all four of the iBypass Switch's ports, and to configure the speed and mode of 10/100/1000 copper ports. (It is important to turn off Auto-Negotiation and set the correct port speed if you are using the iBypass Switch in a fixed-speed copper media environment.)


**Figure 10: The Set Port Parameters button brings up the Port Settings dialog**

## Taking BIG-IP ASM Offline

One benefit of deploying BIG-IP ASM with an iBypass Switch is that BIG-IP ASM can be taken offline, without taking down the link, by issuing a software command to the iBypass Switch from a remote location. (As mentioned previously, the command to force the iBypass Switch into Bypass On mode, taking the BIG-IP ASM offline, is to set the Heart Beat Timeout Period to 0.) This capability can be valuable when putting a new rule set online; if it does not behave as expected, and has a negative impact on a critical business application, BIG-IP ASM can be taken out of the link instantly by forcing the iBypass Switch into Bypass On Mode.

Another feature of the iBypass Switch is that when it is in Bypass On mode, it does more than just issue Heartbeat packets to check the health of BIG-IP ASM. It also acts as a network Tap, mirroring all of the traffic received at network Port A onto monitor Port 1, and all of the traffic received at network Port B onto monitor Port 2. Using this feature, BIG-IP ASM can process the traffic out of band so rule sets can be tested in a non-blocking mode.

The fact that the iBypass Switch acts like a network Tap when it is in Bypass On mode also means that it can be used as a Tap: BIG-IP ASM can be disconnected and a different type of monitoring tool can be attached when needed to investigate a network issue, without impacting the link traffic. There is no need to wait for a maintenance window, get a configuration change approved, or reconfigure a switch for Span.

# Summary

Whether deploying BIG-IP ASM to satisfy the requirements of PCI DSS Section 6.6, or to defend against sophisticated Web application attacks such as SQL injection, URL tampering, or cross-site scripting, you want a solution with maximum reliability to keep your critical business applications up and running at peak performance. Installing BIG-IP ASM with a Bypass Switch device such as the Net Optics 1 GigaBit iBypass Switch provides an extra layer of reliability that protects against power failure and any other condition that may cause BIG-IP ASM to be unable to process traffic. In addition, the 1 GigaBit iBypass Switch provides these benefits:

- Deployment flexibility with media conversion
- Cost saving and convenience with remote device management
- Increased visibility with integrated traffic monitoring
- Peace of mind knowing that BIG-IP ASM can be taken offline at any time with a simple remote software command to the iBypass Switch

Availability of key business applications is critical to your organization's success – that's why you are investing in BIG-IP ASM in the first place. For maximum reliability and peace of mind, we recommend that you consider including a Net Optics iBypass Switch in your BIG-IP ASM deployment.

**F5 Networks, Inc.** 401 Elliott Avenue West, Seattle, WA 98119 888-882-4447 www.f5.com

| F5 Networks, Inc. Corporate Headquarters | F5 Networks Asia-Pacific | F5 Networks Ltd. Europe/Middle-East/Africa | F5 Networks Japan K.K. |
|---|---|---|---|
| info@f5.com | info.asia@f5.com | emeainfo@f5.com | f5j-info@f5.com |


WP-BIG-IP_Net_Optics
© 2009 F5 Networks, Inc. All rights reserved. F5, F5 Networks, the F5 logo, BIG-IP, VIPRION, FirePass, and iControl are trademarks or registered trademarks of F5 Networks, Inc. in the U.S. and in certain other countries. Net Optics, iBypass, Heartbeat, and Indigo are trademarks or registered trademarks of Net Optics, Inc. in the U.S. and in certain other countries.