

Increase Application Availability with External Bypass Switches

Contents

- Introduction 1
- Bypass Switch Operation 1
- Real-World Example 2
- Failover Operation..... 2
- Power Loss Detection 2
- Link Loss Detection..... 3
- Device Management 3
- Conclusion 4

Introduction

TippingPoint Intrusion Prevention Systems (IPS's) are designed to the highest reliability standards so customers can deploy them in-band in their networks without worrying about adversely impacting the availability of mission-critical business applications. In fact, in a survey commissioned by TippingPoint and conducted by Infonetics Research in August 2008, respondents reported that more than 90 percent of all TippingPoint IPS appliances are deployed in-band, a strong indication of the reliability of TippingPoint devices. (In contrast, customers of IPS vendors Cisco Systems, IBM-ISS, and McAfee reported less than 70 percent in-band deployments.)

An IPS must be deployed in-band so it can intercept malicious traffic; if the IPS doesn't have power, no traffic can flow through the link, shutting down the network if redundant connectivity is not available. To remedy this situation, some IPS models have Zero Power High Availability (ZPHA) circuitry built in. This circuitry, often called a bypass switch, automatically opens the link when the unit does not have power, ensuring that network traffic can flow at all times. If an IPS does not include a built-in bypass switch, an external bypass switch may be used, and is recommended for most IPS deployments. In fact, an external bypass switch brings additional value to the solution, because it also keeps the link traffic flowing if the IPS is removed for maintenance or redeployment, or if the IPS or one of its links fails. This paper looks at how an external bypass switch can increase application availability in an IPS deployment, and how such a solution can be installed and configured.

Bypass Switch Operation

A bypass switch, whether internal or external to the IPS, is a device that is designed to provide a fail-safe

connection for in-band equipment such as IPS's. As shown in Figure 1, the external bypass switch is installed in-band in the network link, and the IPS attaches to the bypass switch.

In normal operation, the bypass switch routes all network traffic through the IPS, and the IPS performs its inspection and filtering function in its usual manner, exactly as if the IPS were directly in-band itself.

The bypass switch, however, has the capability of bypassing the IPS and passing traffic directly through the link as shown in Figure 3.

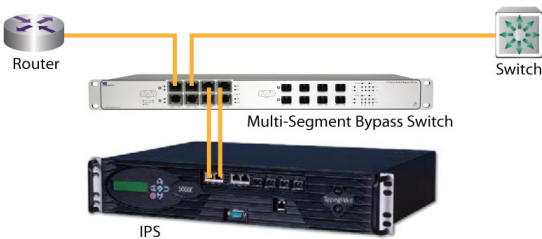


Figure 1: IPS deployed with an external bypass switch

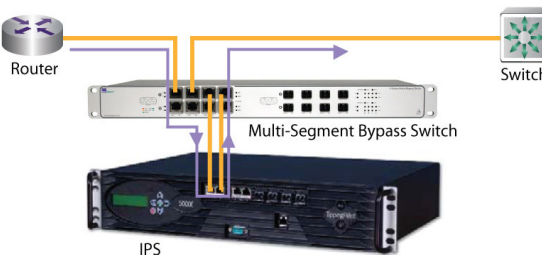


Figure 2: IPS functions as if in-band

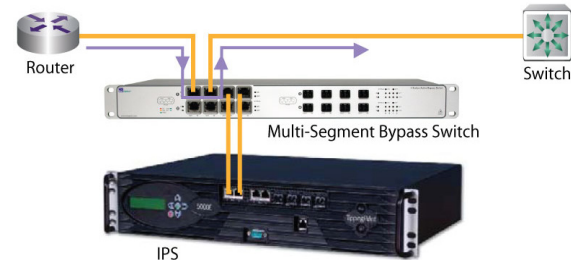


Figure 3: Bypass switch takes IPS out-of-band

One scenario in which the bypass switch will take the IPS out-of-band is if the IPS loses power, and therefore cannot process network traffic. For this reason, an external bypass switch is recommended if the IPS is not equipped with one internally. In addition, when an IPS is paired with an external bypass switch, the IPS can be removed from the link at any time; the bypass switch senses the absence of the IPS and instantly opens the network link to traffic flow.

While the benefits of a bypass switch are evident, you may wonder whether you are simply replacing one risk with another, because the bypass switch is subject to failure as well. However, having a bypass switch in-band has several advantages:

- The bypass switch, whether internal or external, ensures that link traffic continues to flow when no power is available
- A bypass switch is a much simpler device than an IPS, so it is less likely to fail
- A bypass switch passes 100 percent of the network traffic, no matter how busy the link is; it never runs out of bandwidth and therefore never needs to be upgraded
- External bypass switches are often installed in critical links as permanent parts of the network infrastructure, so they never need to be removed from links, even when the security strategy or the network configuration changes

A Real-World Example

A perfect companion bypass switch for TippingPoint 5000E and 2400E IPS's (which do not have internal bypass switches) is a Net Optics Four-Station Multi-Segment Bypass Switch. Both devices support four network links, and both can be ordered in configurations with all copper, all fiber, or half copper and half fiber ports. Both SX and LX fiber are supported. The two devices can be paired as shown in Figure 4.

This configuration protects four critical network segments and occupies only 3U of rack space, 2U for the IPS and 1U for the Bypass Switch.

For example, a TippingPoint 2400E appliance is often a good choice to protect four 1-gigabit-per-second network links if the links are less than 50 percent utilized. However, suppose that over time network usage grows and the 2-gigabit-per-second aggregate throughput capability of the 2400E becomes a bottleneck on the network. A properly managed network may function well at utilizations of 80 percent or more, so it may be possible to continue to meet service-level agreements without upgrading the network—except that the IPS no longer has the bandwidth to handle all of the traffic. The most cost-effective solution may be to upgrade from a

2400E to a 5000E, which supports 5 gigabits per second of throughput. If the 2400E was deployed with a Multi-Station Bypass Switch, upgrading is a cinch. The cables are simply unplugged from the 2400E (the Bypass Switch automatically and transparently keeps the network traffic flowing), the 5000E is swapped for the 2400E in the rack, and the cables are plugged into the 5000E. As soon as the 5000E is powered up and is capable of passing traffic, the Bypass Switch automatically switches it in-band and the network is protected. There is no need to wait for a maintenance window or worry about impacting application traffic.

Failover Operation

Let's take closer look at how an external bypass switch keeps the traffic flowing.

The Net Optics Multi-Station Bypass Switch has three mechanisms for triggering a bypass, that is, for taking the IPS out-of-band. The mechanisms are power loss detection, link loss detection, and Heartbeat packet. Each of these mechanisms is described in the following sections.

Power Loss Detection

The Multi-Station Bypass Switch has dual redundant power supplies and ZPHA circuitry that detects loss of power. When the dual redundant power supplies are connected to independent power sources, total loss of power should be rare, because either power supply alone can power the unit. However, when both power sources fail, the ZPHA circuitry ensures that the Bypass Switch creates an open channel that enables network traffic to keep flowing while the Bypass Switch has no power. When power is restored, the Bypass Switch automatically comes back on-line and, if the IPS is detected to be present and functioning, restores the flow of network traffic through the IPS.

The Tolly Group conducted independent tests on a Net Optics Bypass Switch (10/100/1000 copper model) in April 2008. They reported the

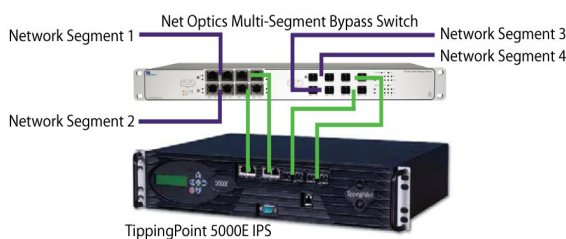


Figure 4: TippingPoint 5000E IPS paired with a Net Optics Multi-Segment Bypass Switch

time from a power fail condition on the Bypass Switch to when the network connection was re-established and traffic resumed flowing to be 0.82 seconds.

Link Loss Detection

The Multi-Station Bypass Switch monitors the links between its ports and the IPS. If a link is dropped, the switch immediately enters “bypass on” mode taking the IPS out-of-band and enabling traffic to flow unimpeded through the link. The Tolly Group induced this condition by unplugging one of the cables that connected the Bypass Switch to the IPS, and measured a failover time of 0.76 seconds. This test reflects the real-world scenario wherein the IPS is removed from the network for any reason, and demonstrates that application traffic keeps flowing when the IPS is simply unplugged and removed.

A third method of triggering a “bypass on” condition is required for cases when the Bypass Switch remains powered and the links to the IPS remain up. An example of this scenario is when the traffic exceeds the capacity of the IPS, so that latencies through the IPS start to increase. To detect this type of condition, the Bypass Switch periodically sends small Heartbeat packets through the IPS to confirm that it is operational. The Heartbeat packets are sent out one port to the IPS, and the Bypass Switch expects to see the packet returned on the other port within a certain amount of time. If the packet does not arrive within the expected time window, the Bypass Switch assumes the IPS is having a problem and takes it out-of-band. (The Heartbeat packet is received by the Bypass Switch but it is never passed to the external network link.)

The Tolly Group tested the Heartbeat packet mechanism by programming the IPS to filter the Heartbeat packet, so it would not be returned to the Bypass Switch. They determined that in this scenario, the failover time was less than one millisecond.

Device Management

TippingPoint IPS’s are quick and easy to deploy. Forty-two percent of TippingPoint customers in the previously referenced Infonetics Research survey reported installing the IPS in less than 30 minutes, and 76 percent in less than two hours. (For comparison, only 17 percent of IBM-ISS customers reported a two-hour or less set-up time.) In addition, two-thirds of TippingPoint customers said that only a light effort was required to configure the IPS filters, and only three percent said it took significant effort.

Some customers may wish to adjust some of the Bypass Switch’s configurable features for their application. Bypass Switch configuration is easily accomplished with a command-line interface (CLI) operating over an RS232 serial port. The Multi-Segment Bypass Switch has a separate RS232 port for each of the four segments, because the Bypass Switches that control the segments are completely independent from each other for added reliability and security.

The configurable features of the Bypass Switch include the following:

- **Link Fault Detect (LFD)** – disables the remaining side of a full-duplex link when one side of the link fails, ensuring that the network can failover to an alternate path (if available) in a timely manner; the default setting for LFD is **On**
- **Bypass Detect** – when in “bypass on” mode, Bypass Detect cycles the monitor ports through five seconds off followed by ten seconds on; the resulting alternating link status can trigger the attached IPS to send an alarm to a management system; Bypass Detect activates when the Heartbeat packet is not returned from the IPS device; the default setting of Bypass Detect is **Off**
- **Fail Mode** – When the Fail Mode setting is “open,” the “bypass on” state of the switch is to open the network link and permit

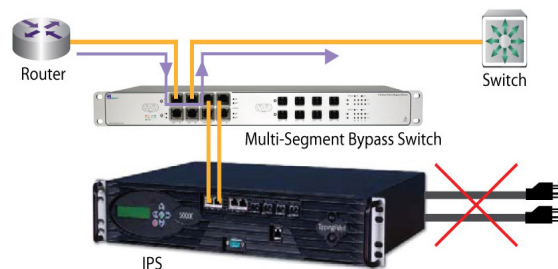


Figure 5: Bypass triggered by loss of power to the Bypass Switch

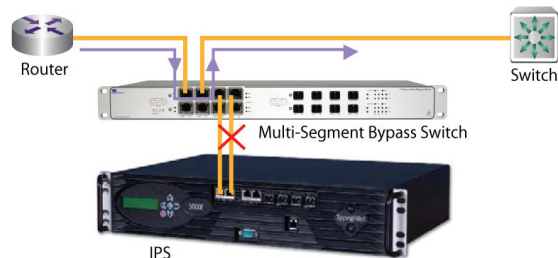


Figure 6: Bypass triggered by loss of link between the IPS and the Bypass Switch

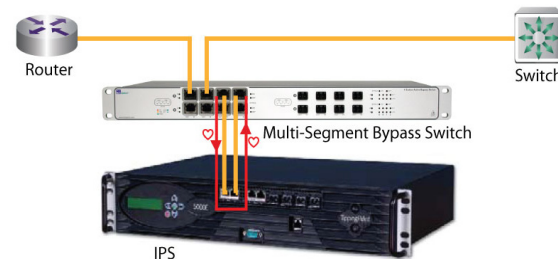


Figure 7: Operation of the Bypass Switch Heartbeat packet

traffic to flow, as discussed previously; when the setting is “closed,” the “bypass on” state closes the network link so no traffic flows, enabling failover network settings to take effect; the default setting for Fail Mode is **Open**

In addition, 10/100/1000 copper-media ports can be configured to a fixed speed of 10, 100, or 1,000 megabits per second, and to full or half duplex mode. The default settings are automatic negotiation of link speed, and full duplex mode.

The Bypass Switch’s Heartbeat packet is also configurable. Besides the actual packet content, the interval between Heartbeat packets and the retry count may be configured. The default interval between Heartbeat packets is one second; it can be set from 1 to 254 seconds. The default retry count is three, meaning that the Bypass Switch takes the IPS out-of-band when three Heartbeat packets have failed to be returned. The retry count can be set from 1 to 254. The default Heartbeat packet configuration works well with Tipping Point 5000E and 2400E IPS’s.

The status of the links and the bypass state of the Multi-Segment Bypass Switch can be viewed through the CLI. It is also shown with LEDs on the device’s front panel. Each of the four independent switches has a pair of LEDs that show whether the state is “bypass on” (IPS out-of-band) or “bypass off” (IPS in-band). In addition, each port has two LEDs displaying the link state: a Link LED that indicates whether the link is present or not, and an Activity LED that flashes when data is passing through the port. For 10/100/1000 ports, the color of the Link LED also indicates the link speed, amber for 10 megabits per second, yellow for 100 megabits per second, and green for 1,000 megabits per second, as clearly explained with a key silkscreened on the panel. Finally, each of the four switches has a pair of LEDs indicating whether the two redundant

power supplies are active or off.

If remote management of the Multi-Segment Bypass Switch is desired, an inexpensive four-port RS232 terminal server can be obtained from any of a number of sources to enable access to the management ports over a network or over the Internet.

Conclusion

TippingPoint IPS’s are designed for maximum reliability, with features such as redundant configurability, link down synchronization, and hardware watchdogs. However, availability of business-critical applications can still be affected when an IPS needs to be removed from a network link or upgraded to a new model. An external ZPHA or bypass switch ensures a higher level of application availability by guaranteeing that link traffic keeps flowing in all of these scenarios. A Net Optics Four-Station Multi-Segment Bypass Switch is an ideal companion for TippingPoint 5000E and 2400E IPS’s because together they can protect four critical network links with as much as 5 gigabits per second of total traffic, with high reliability and the flexibility of being able to remove or upgrade the IPS’s at any time, without risking the availability of critical business applications.



Figure 8: Net Optics Multi-Segment Bypass Switch Front Panel

Corporate Headquarters:

7501B North Capital of Texas Hwy.
Austin, Texas 78731 USA
+1 512 681 8000
+1 888 TRUE IPS

European Headquarters:

Herengracht 466, 2nd Floor
1017 CA Amsterdam
The Netherlands
+31 20 521 0450

Asia Pacific Headquarters:

47 Scotts Road
#11-03 Goldbell Towers
Singapore 228233
+65 6213 5999

TippingPoint

www.tippingpoint.com