



Check Point IPS-1 and Net Optics Bypass Switches

External Bypass Switches add an extra layer of protection



Contents

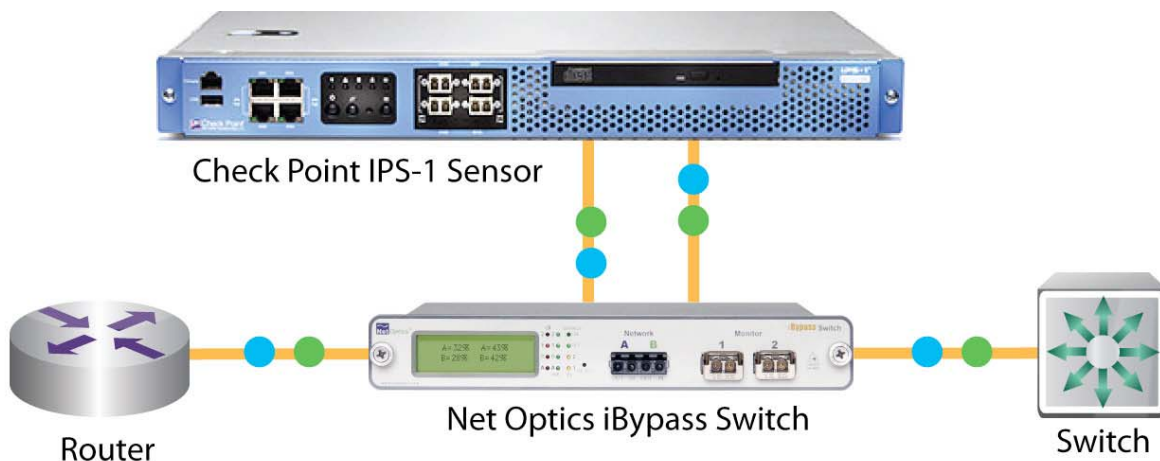
Overview.....	2
Failover operation	4
Benefits of an external Bypass Switch	5
Configuring the iBypass Switch.....	6
Heartbeat packet options	6
Configuring the ports	8
Taking IPS-1 offline.....	8
The Net Optics iBypass Switch family	8
Summary	10

Overview

Check Point IPS-1 is the leading solution for dedicated enterprise-scale intrusion prevention. When deploying IPS-1 Sensors inline, it is important to consider what happens if the device loses power, is taken offline, or experiences any type of failure.

IPS-1 Sensors may be deployed in a redundant configuration, with a backup unit that takes over when a failure occurs. While this solution keeps IPS security highly available, it adds the cost of redundant sensors to the solution. An alternative is to deploy the IPS-1 Sensor singly, with a hardware failover circuit to ensure that the device fails either unsevered or severed, depending on your policy. Unsevered failover, where traffic passes through the hardware failover circuit, keeps traffic flowing and critical business applications available, though without IPS security. Severed failover, where network link is severed when IPS-1 cannot process the traffic, is appropriate when security is more important than traffic flow.

All IPS-1 Sensors contain hardware failover circuits that can be configured for unsevered or severed operation, ensuring that your security and traffic flow policy is enforced even in power loss or other failure conditions. However some customers choose to deploy IPS-1 Sensors with external failover circuits, called Bypass Switches, for an extra level of protection and versatility. This paper looks at the benefits of using an external Bypass Switch with IPS-1 Sensors. The solution is illustrated with a Net Optics iBypass Switch, which is OPSEC-certified by Check Point Software Technologies.



Failover operation

A pass-through hardware failover circuit ensures that traffic keeps flowing (for an unsevered failover policy) when IPS-1 cannot process the traffic for any reason. Figure 1 illustrates traffic flowing through the IPS-1 processing unit when it is operating normally (Bypass Off mode).

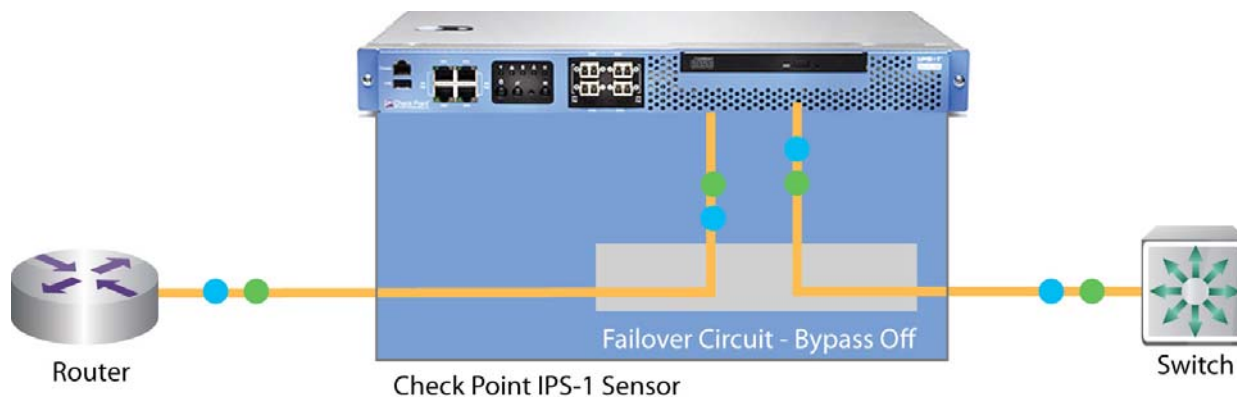


Figure 1. Failover circuit normally directs traffic through IPS-1 processing

Figure 2 illustrates traffic passing directly through the failover circuit when failover is engaged (Bypass On mode), either because of loss of power or any other failure condition.

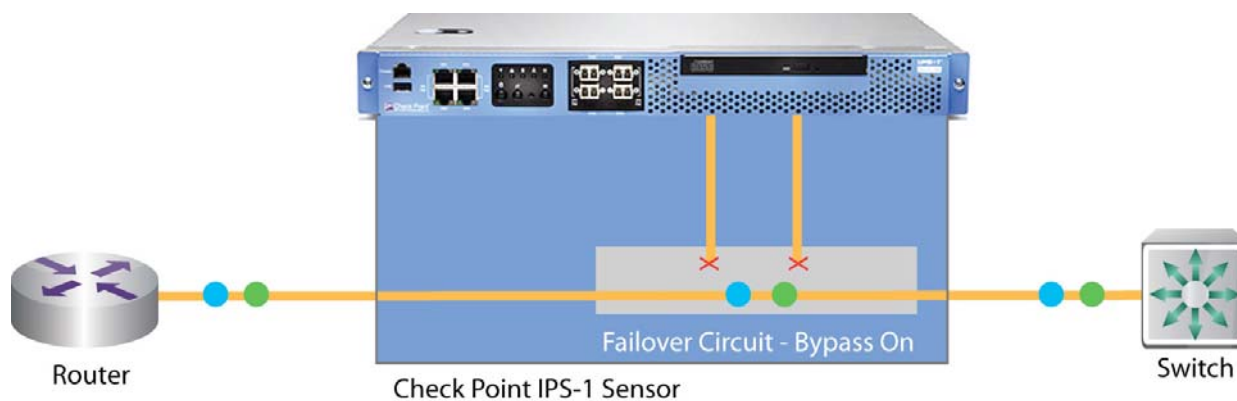


Figure 2. Upon failure, failover circuit passes traffic directly, bypassing IPS-1 processing

The same functionality can be provided with an external Bypass Switch, providing the benefits described in the following section.

Benefits of an external Bypass Switch

Using an external iBypass Switch provides several benefits:

- An external iBypass Switch adds an extra measure of reliability because it is a totally independent check on IPS-1. The iBypass Switch periodically sends a small Heartbeat packet through IPS-1 to verify its functionality; if the Heartbeat packets are not returned within a configurable timeout period and retry count, IPS-1 is judged to be non-responsive and Bypass On mode is entered. The iBypass Switch continues to send Heartbeat packets to IPS-1, and when it becomes responsive again, the bypass is automatically switched off and traffic is once again routed through IPS-1.

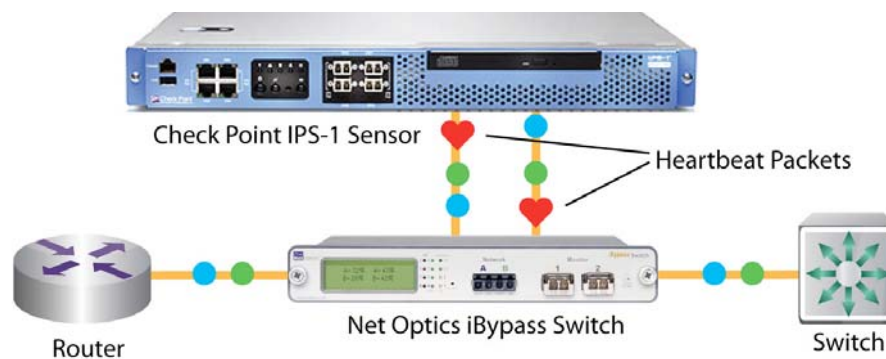


Figure 3. iBypass Switch monitors IPS-1 health with a Heartbeat packet

- An external iBypass Switch adds flexibility to the deployment because IPS-1 can be removed for upgrade or maintenance without disturbing network traffic. Furthermore, the iBypass Switch can be remotely commanded to take IPS-1 offline whenever desired; for example, when testing new rule sets. In addition, the device behaves like a standard Network Tap when in Bypass On mode, mirroring the network traffic to the two IPS ports, so it can actually be used as a Tap when desired.
- An external iBypass Switch adds additional instrumentation. The iBypass Switch provides RMON traffic statistics on all of its ports, so traffic passing through IPS-1 as well as through the network link can be monitored independently of IPS-1. RMON statistics can be viewed on the LCD display on the front panel of the iBypass Switch, or remotely using Indigo™ device management software provided by Net Optics, or with any SNMP-based management tool such as IBM Tivoli or HP OpenView.



Figure 4. RMON traffic statistics displayed on the iBypass Switch front panel

Many organizations feel that the increased reliability, flexibility, and instrumentation provided by the iBypass Switch more than justify the cost of the device in their overall IPS-1 solution.

Configuring the iBypass Switch

The iBypass Switch is designed for simple plug-and-play installation; just plug it into the network, connect IPS-1 and power, and it is fully functional. However, you may choose to reconfigure some of the iBypass Switch settings to tune it for your particular environment. The iBypass Switch can be configured using a text-based command-line interface (CLI) using a terminal emulator operating over a serial port. It can also be configured using Net Optics-supplied Indigo software, which includes a Web browser based tool called Web Manager and a platform (Windows) based tool called System Manager.

Heartbeat packet options

Figure 5 shows the lower part of the main Web Manager page for the iBypass Switch. At the bottom of the screen, below a variety of other configurable parameters, 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 IPS-1 Sensor. The default timeout is 1 second, but it can be increased if this isn't enough time, for example if IPS-1 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.

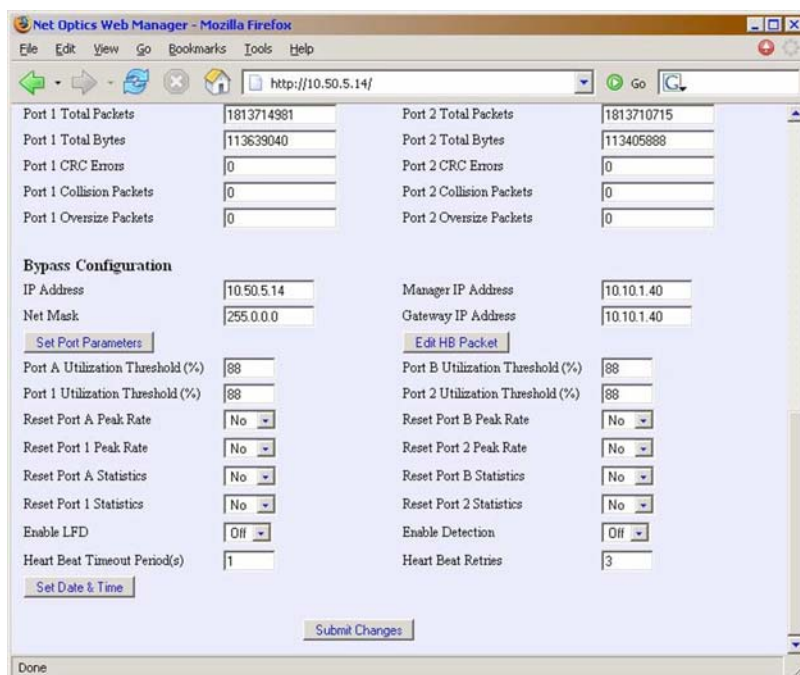


Figure 5. Web Manager configuration section

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 the IPS-1 Sensor 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 IPS-1. 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 on the Refresh the Packet list and click Apply to refresh the displayed packet.)

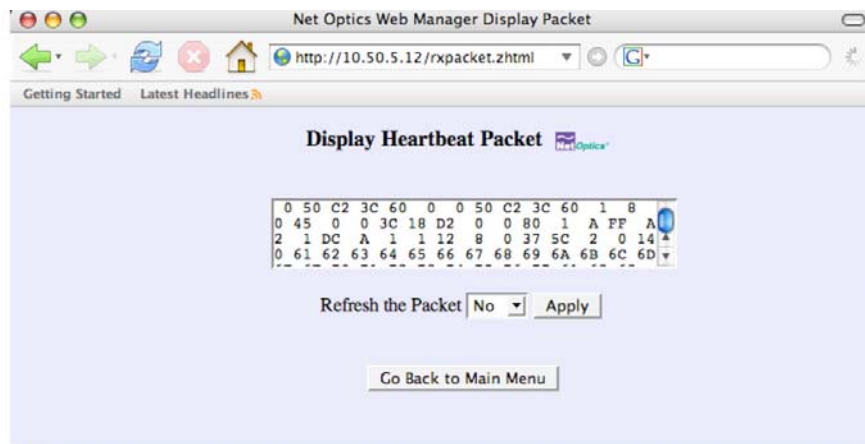


Figure 6. Web Manager displays the current Heartbeat packet values

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.)

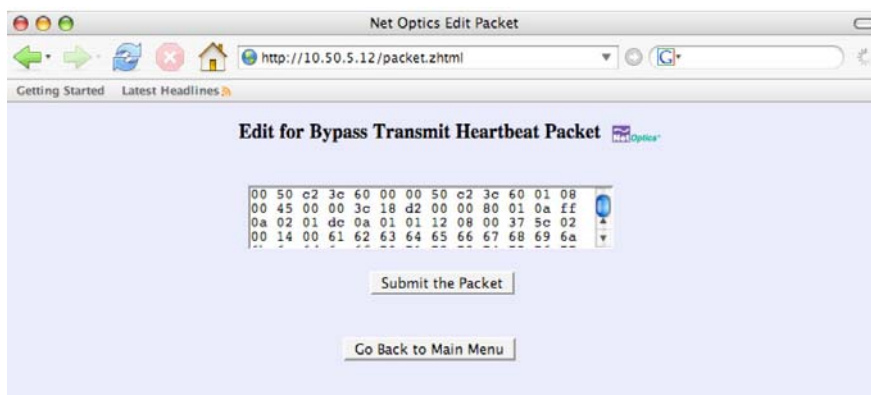


Figure 7. Web Manager enables the Heartbeat packet contents to be changed

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 8. The Set Port Parameters button brings up the Port Settings dialog

Taking IPS-1 offline

One benefit of deploying IPS-1 with an iBypass Switch is that IPS-1 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 IPS-1 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, IPS-1 can be taken out of the link instantly by forcing the iBypass Switch into Bypass On Mode.

The Net Optics iBypass Switch family

The Net Optics iBypass Switch is a versatile external Bypass Switch for IPS-1 deployments. It is available for both copper and fiber networks, with speeds from 10/100/1000 Mbps to 10 Gbps. On fiber models, the ports that connect to IPS-1 take modular SFP and XFP transceivers enabling media conversion; for example, a 1 Gigabit fiber network can utilize less expensive copper media to connect IPS-1 and the iBypass Switch. In addition, the iBypass Switch can operate from a single power supply or dual redundant supplies for increased reliability. Net Optics also supplies Multi-Segment Bypass Switches with four independent Bypass Switches in a 1U chassis, and Bypass Switches without remote management capability. Net Optics iBypass and Bypass Switches are compatible with IPS-1 and other Check Point inline appliances sensors.

Net Optics iBypass Switch Family

Model	Speed	Network ports	IPS ports
iBP-HBCU3	1 Gigabit	10/100/1000 Copper	10/100/1000 Copper
iBPO-HBSX-SFP	1 Gigabit	SX (Multi-mode) Fiber	SFP (SX, LX, or Copper)
iBPO-HBLX-SFP	1 Gigabit	LX (Single-mode) Fiber	SFP (SX, LX, or Copper)
iBPO-HBSR-XFP	10 Gigabits	SR (Multi-mode) Fiber	XFP (SR or LR)
iBPO-HBLR-XFP	10 Gigabits	LR (Single-mode) Fiber	XFP (SR or LR)



Figure 9. Net Optics iBypass Switch



Figure 10. Net Optics Multi-Segment Bypass Switch



Figure 11. Net Optics Bypass Switch without remote management

Summary

When deploying an IPS-1 Sensor in a configuration without a redundant backup unit, the IPS-1 internal failover circuit can be supplemented with an external Bypass Switch such as the Net Optics iBypass Switch. The external Bypass Switch can provide an extra layer of reliability to protect against any condition that might prevent IPS-1 from passing traffic. In addition, the iBypass Switch provides these benefits:

- Deployment flexibility with media conversion and the ability to remove IPS-1 from the link without disrupting traffic
- Cost saving and convenience with remote device management
- Increased visibility with integrated traffic monitoring
- Peace of mind knowing that IPS-1 can be taken offline at any time with a simple remote software command to the iBypass Switch

When protecting key business applications with IPS-1 security, an investment in external Bypass Switches can pay dividends and increase the ROI of your overall security solution.