Fail-Safe IPS Integration with Bypass Technology

Summary

Threats that require the installation, redeployment or upgrade of in-Line IPS appliances often affect uptime on business critical links. Organizations are demanding solutions that prevent disruptive outages and provide an efficient return on investment for their IPS resources.

Net Optics offers intelligent bypass solutions for a secure in-Line deployment with remote control and monitoring. The iBypass Switch with Heartbeat™ technology protects against power, link, and application loss.

SNMP and Web browser interfaces allow for remote management, providing access to baseline traffic statistics, alarms and utilization levels.

Table of Contents

White Paper

NetOptics
an ixia company

Fail-Safe IPS Integration with Bypass Technology

White Paper

Key Features

- Secure monitoring with any in-Line appliance
- Protects against downtime due to power, link, and application failure
- Maintains link integrity during IPS redeployments and upgrades
- Remote control and monitoring from Web browser and SNMP interfaces
- Front panel LCD shows traffic utilization levels and peaks
- View basic traffic counters from remote interfaces

Introduction

The growth of the Internet is driving the need for global networks to connect businesses, organizations, and individuals together. The need to control and protect the flow of information has dramatically increased as well. Malicious and unpredictable attacks have become commonplace and have blurred the lines of responsibility between IT network and security organizations. As a result, both groups often deploy separate tools and monitoring devices on the same important, business-critical network links.

Firewalls are security control points that can be either standalone devices or embedded in network routing equipment. Firewalls operate by applying a set of rules whereby packets are checked as they pass through the network. Since the networking team usually manages firewalls, the security team is often challenged in its efforts to stay abreast of changes to the network and the rules being applied. As threats and viruses became more prevalent and transparency became an issue, the need for more sophisticated and targeted security devices conflicted with the analysis equipment used by the network team.

Intrusion-prevention system (IPS) appliances were developed to provide security teams with a device that could be placed in the direct flow of traffic within network links. An IPS not only notified network security administrators of suspicious activity, but could also respond to that activity by manipulating or blocking traffic. These devices were an improvement over firewall security measures because the IPS appliances allowed security managers to make real-time decisions based on application content rather than by IP address or port. Furthermore, most IPS appliances allow physical layer protocols and encrypted traffic to be monitored.

> The NSS Group states “IPS are proactive defense mechanisms designed to detect malicious packets within normal network traffic…and stop intrusions dead. Blocking the offending traffic automatically before it does any damage rather than simply raising an alert…”(1)

The Challenge

Regardless of the type of monitoring device being placed in-line within a network link both the network and security teams encounter similar issues. Network outages and downtime are required to install a monitoring device, and if it fails or needs to be moved, the physical stream is once again interrupted. For most, introducing a recognized, potential point of failure into the network is a truly unacceptable solution.

Creating a solution that addresses the concerns and connectivity issues experienced by both the network and security teams within an organization has become increasingly critical.

Industry Response to IPS Concerns

In response to these issues, the monitoring appliance vendors turned to Tap vendors to satisfy the need for passive in-line devices that help solve the problems that occur due to power loss, IPS malfunction or redeployment of the appliance. A device was needed that could be bundled with monitoring appliances and offered customers a tested solution—the Bypass Switch.

Common features would include dual power supplies, visual status indicators, dual network and IPS monitor ports. And, for optimum performance, a means to capture and provide reports on the health of the network would be essential.

The Net Optics Solution

Bypass Switches were created to remain in-line, copy traffic to the IPS, provide a path for the IPS to manipulate traffic, and maintain link continuity. Innovation came about by looking at the problem from multiple perspectives and combining features that address the following problems:

- The results of power loss at the Bypass Switch
- Power loss at the IPS
- The appliance being taken off-line for maintenance
- The effects of heavy traffic

More recently, Net Optics, Inc. broadened the control functions of its switches by incorporating intelligent technology into the iBypass Switch, providing network security administrators with access to links and devices from remote locations and even greater visibility into operations via real-time statistics.

Features That Deliver

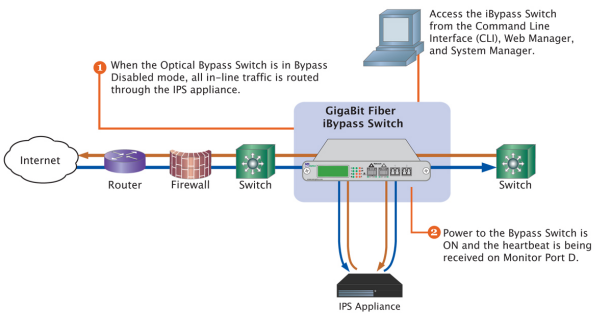
Based on passive, fail-open technology that regularly monitors traffic flow, iBypass Switches help security managers quickly identify link anomalies or device failures. Automated functionality ensures that information forwarded to an IPS is correct or not sent at all.

Heartbeat™

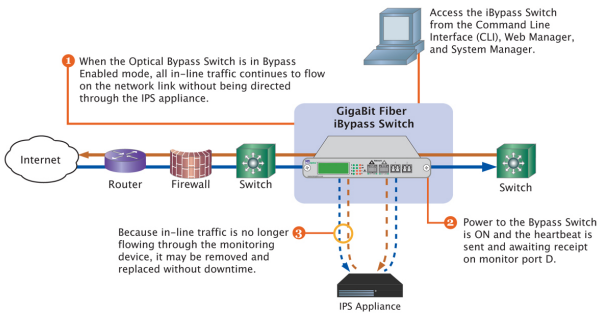
The “Heartbeat” feature sends customer-configurable packets to the IPS appliance continually verifying the state of the link between the IPS and the Switch. The frequency of the heartbeat and the type of heartbeat packet are customizable depending on appliance and network type. If the Bypass Switch does not receive a response packet from the IPS in a timely manner, the Switch becomes enabled (Bypass Mode) and reroutes traffic away from the IPS. As a result, security engineers have greater visibility into traffic loads and are assured improved reliability in the network.

> “By transmitting and successfully receiving heartbeat packets in the proper time frames, the Bypass Switch knows the monitor device is properly functioning.”(2)

iBypass w/Heartbeat Switch Disabled Mode



iBypass w/Heartbeat Switch Enabled Mode



Fast Path™

All models incorporate Fast Path switching technology for minimized packet loss in the event bypass mode is enabled. Once an iBypass Switch is placed in-line and the IPS is connected to the switch, if a link

failure is detected, the switch routes traffic through the switch rather than to the non-functioning link. If an IPS device ceases to function, the iBypass Switch automatically, and without disruption, routes network traffic, effectively bypassing the monitoring device.

Software Management Tools

The iBypass Switch also provides a spectrum of management tools that help to view and obtain statistics and control hardware from multiple locations. Basic network statistics and functions are accessible through the command line interface (CLI). However, intelligent IP and SNMP features enhance remote management operations through the use of *Web Manager, System Manager, and Management Information Base* tools.

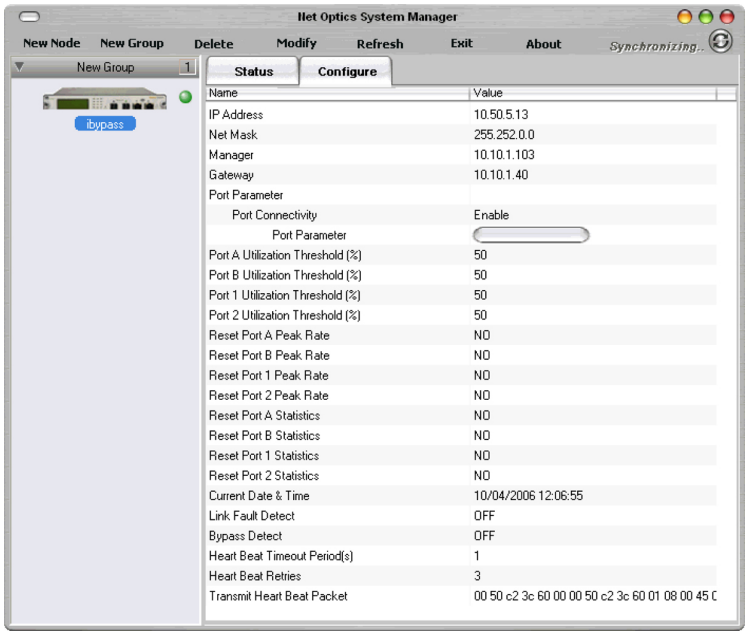
> Volumes of alert data and frequent false positives are significant issues for networks deploying gigabit products. “More than ever before in the IDS space, centralized management reporting and forensic analysis is key to the success of the Gigabit appliance.” (3)

Web Manager is a browser-based tool that allows for the management of singular devices. No specialized software is required to change settings, view status, or change port connections.

The *System Manager* is a centralized software management tool that can be configured to access all intelligent devices in the network enabled by simple network management protocol (SNMP). All iBypass Switches and iTaps can be grouped for optimum organization and easy monitoring. System Manager allows security administrators to view all status, configuration, and traffic information in real-time, as well as to quickly make changes to any switch or tap in the network.

Organizations with existing SNMP tools in place or who wish to use an industry standard SNMP management platform can integrate the Net Optics *Management Information Base* into their own software.

These software tools allow security managers to see into their networks as well as make changes from remote locations thereby providing easy access and control to the numerous links in the network. Engineers can now monitor and troubleshoot from a central location to keep the network up and running smoothly while the enterprise operates securely and efficiently.



Hardware Functionality

The failsafe, in-line technology available via iBypass Switches maintains seamless traffic flow when connected to the same power source as the IPS—the traffic is not interrupted in the event of power loss.

The front panel display and threshold alarm LEDs provide a continuous verification that utilization levels are not exceeding capacity of the IPS or a pre-determined level, or that an event has taken place that

needs to be investigated. An LED shows whether traffic is going through the IPS or bypassing the IPS through the switch. Additional LEDs show power, speed, link, and activity status. Network utilization detail is important for seamless, reliable transmission of data throughout organizations. The added functionality in Net Optics iBypass Switches makes statistics about the physical stream available on a continuous basis—byte counts, individual packet characteristics, packet size, and packet collisions. Packet loss, transmission latency, and errors identified by cyclic redundancy checks (CRC) are recorded as well.

Net Optics iBypass Switches are available with copper or fiber optic interfaces for high-speed (Gigabit) networks. The 10/100/100BaseT iBypass is compatible with copper-based networks and monitoring devices. The GigaBit SX iByPass Switch incorporates SX and LX fiber optics interfaces.

Enhanced Information Visibility

Network information available from the front panel display, CLI, Web Manager, and System Manager includes the percent of network utilization, physical layer statistics, link activity, and power status to switches. The iBypass Switches have an early warning system—threshold alarms that are visible on the front panel as LEDs and sent through the network to alert managers of bypass events.

When All Else Fails

In today's business-critical environments, 24/7 link uptime is not an option. It is a strategic imperative. The Net Optics iBypass Switches can be used in-line to protect critical links from downtime when disruptive power, link, or application events occur. The iBypass Switch provides a permanent, flexible, and secure solution to minimize threats across the network.

Next Steps

To find more about Net Optics solutions, please visit
http://www.netoptics.com

References

1. NSS Intrusion Prevention Systems (IPS), January 2004. Retrieved April 2007 from: http://www.nss.co.uk/WhitePapers/intrusion_prevention_systems.htm
2. Bejtlich, Richard, April 2007, Bypass Switches Competitive Review, www.TaoSecurity.com
3. NSS Gigabit Intrusion Detection Systems (IDS), January 2004. Retrieved April 2007 from http://www.nss.co.uk/WhitePapers/gigabit_ids.htm

For further information on Tap technology:

http://www.netoptics.com/support/whitepapers

Net Optics, Inc.
5303 Betsy Ross Drive
Santa Clara, CA 95054
(408) 737-7777
info@netoptics.com
www.netoptics.com

Customer First!