External Bypass Switches

A Better Inline Security Solution

FOR EVERY NETWORKING TOOL

Keeping network and security tools alive on any size network.

The Need for Bypass Functionality

For perimeter security, many organizations turn to an inline security strategy as a first line of defense. Intrusion-prevention system (IPS) appliances provide security and IT teams with a device "inline" with the direct flow of traffic.

These devices are 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 more basic data.

The need to control and protect the flow of information has dramatically increased as well. In a recent survey, 35% of companies reported experiencing network downtime due to a security attack, and 52% of attack-related downtime resulted in more than one hour of outage.

When a network monitoring device such as an IPS is deployed inline in a network link, it is vital to ensure that traffic continues to flow in all circumstances, even if the IPS loses power, so that mission-critical business applications remain available. If the IPS function is crucial to application security, traffic must be switched to a backup IPS device.

A bypass switch is an excellent solution that ensures continued availability.

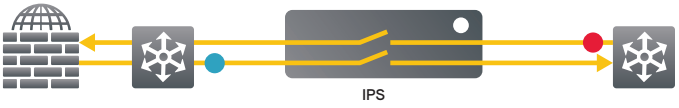
A bypass switch is a passive device that maintains traffic flow when the IPS is not available. There are two basic implementations for bypass switches: internal and external. Internal bypass is performed as a function of an inline security device such as an IPS. The bypass function can also be performed outside the IPS itself, using an external Bypass switch device. For example, Ixia has a line of bypass switch devices that support any link media type and provide a variety of features.

External bypass switching advantages include:

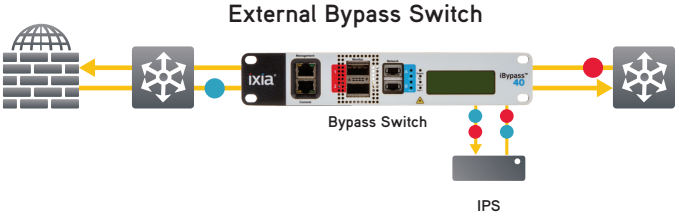
- Increased Security
- Network Reliability
- Better Visibility
- Programmability

This paper examines the value an external bypass switch provides, over and above that of an internal bypass switch. Bypass switches improve the overall solution reliability, increase application availability, provide better instrumentation, and add the convenience and cost savings of remote monitoring and control.

Internal Bypass Switch



External Bypass Switch



Increased Security

Security is at a premium today for both the enterprise and the consumer. The consumer needs to trust the networks they use, and therefore the enterprise must make securing networks a priority in order to maintain business and brand fidelity.

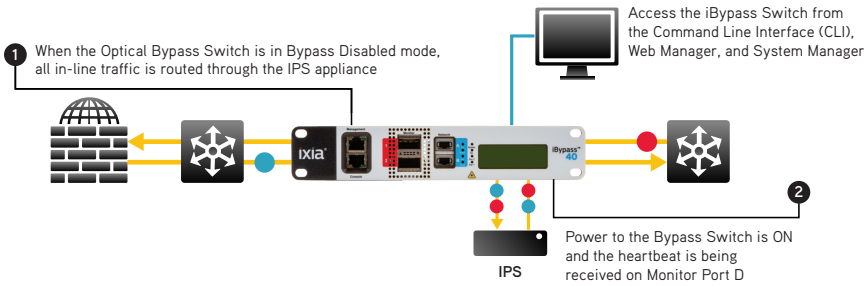
Inline security resources can themselves actually become points of failure and vulnerability. They bring concerns about network uptime, performance, operational ownership, security flexibility and overall costs. Despite redundancy and other protections, they must be taken offline for upgrades and scheduled or unscheduled maintenance. Further, if a tool loses power or becomes overprovisioned, the network link can break and traffic cease to flow.

Bypass switches offers a proven solution for deploying multiple inline security tools. Bypass switch bi-directional heartbeat monitoring for system, link, and power failures ensures uninterrupted network uptime while increasing network availability. Security tool load balancing ensures efficiency while enabling you to leverage existing tool investments and add capacity as needed, rather than investing in a forklift upgrade.

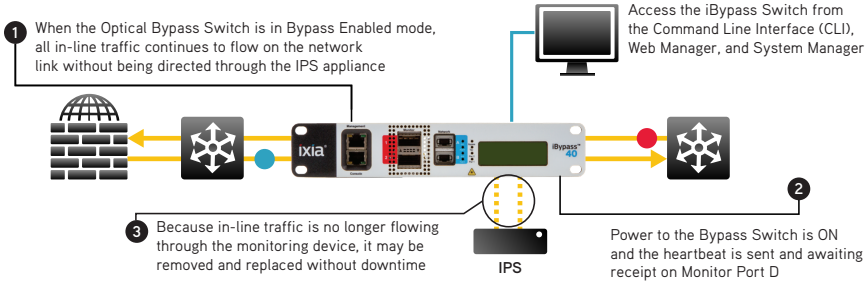
Replacing multiple inline security devices with a single passive bypass switch eliminates network maintenance downtime while providing a pay-as-you-go capacity upgrade path for your changing security needs—dramatically reducing costs of migrating your 1GbE tools to the 10GbE environment, for example.

Ixia bypass switches offer proven, fail-safe inline protection for your security and monitoring tools. With support for 10Mbps to 40Gbps connectivity, you receive automated failover protection on full duplex traffic streams. Because the bypass switch is passive, link traffic continues to flow even if the bypass itself loses power.

iBypass w/Heartbeat Switch Disabled Mode



iBypass w/Heartbeat Switch Enabled Mode



Improved Network Reliability

Anything can fail. The question is never "Will it fail?" but rather "When will it fail?" According to Ixia's survey, hardware failure drove 42% of all network incidents. 53% of network devices are aging or obsolete. Devices WILL fail.

More than 90 percent of our customers prefer availability over security when a security tool fails. An external bypass switch increases the reliability of an IPS deployment because it keeps traffic flowing whenever the IPS fails, for any reason.

The bypass switch can automatically detect an issue with inline tools and route traffic around the security tool while issuing an alert to ensure action is taken by the network or security teams. Internal bypass switches may not have all the technology advantages of an external solution, and therefore simply do not protect your network as well.

An external bypass switch improves the solution reliability by adding an independent check on the IPS, but it also contributes to availability in another way. Using an external bypass switch, you can take an off-line at any time without affecting link traffic.

For example, if you activate a new set of intrusion signatures and the impact on the network is not what was expected— too many false positives show up, blocking critical traffic—you can easily bypass the IPS. In either case, the external bypass switch keeps link traffic flowing. This capability is often not available in an internal bypass switch.

More advanced bypass switch models provide high availability support, allowing customers to configure redundant inline tool infrastructure to maximize availability. Certain models even support simple serial inline deployments where if one tool fails, traffic is automatically rerouted to the next inline tool.

An Ixia Heartbeat Measures the Health of Your Inline Solution

One important technology included in many Ixia bypass switches is the Heartbeat packet. A hearbeat is a small packet that the bypass switch passes through the IPS on a regular basis. If the Heartbeat packet is not returned to the bypass switch within a programmed timeout period (and number of retries), the bypass switch knows the IPS is unresponsive immediately opens the link allowing network traffic to flow directly, bypassing the IPS.

While heartbeats are common to many bypass technologies, Ixia's heartbeat technology is superior to other implementations for two reasons. First, the granularity of the Heartbeat packet can be set to a very high frequency (down to 1 nanosecond). This guarantees that if an inline security device fails, the bypass switch will know nearly instantaneously, and react.

Secondly, Ixia's implementation is based in the bypass field-programmable gateway array (FPGA), not the software. This hardware-based heartbeat means the response time of the bypass switch is also measurable in nanoseconds (between 1 and 3). This translates to very little (if any data) loss by the IPS or other inline security device in the fail over process (or on the network should it fail open).

Visibility

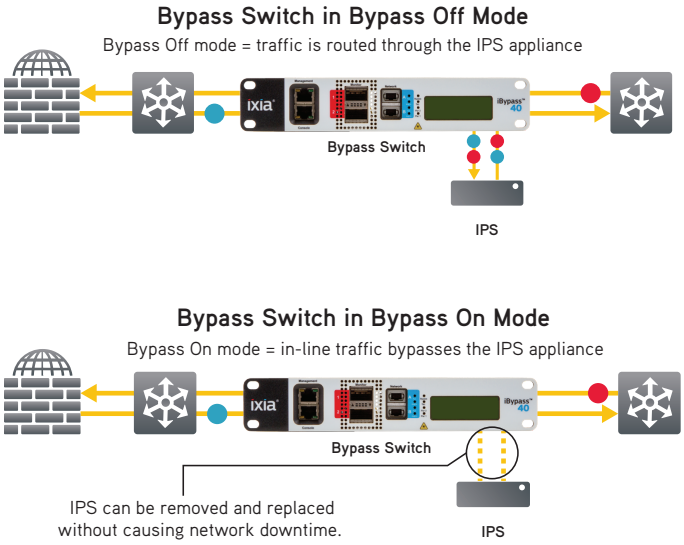
We have seen that a basic external bypass switch improves the overall network reliability and application availability compared to a bypass switch internal to the IPS. However, Ixia offers bypass switches with additional features that add even more value. These products include a remote management interface that enables network professionals to monitor the status of the bypass switch itself, the attached IPS device, and the attached links.

Obtaining traffic statistics from the bypass switch is particularly valuable. Information such as bandwidth utilization, peak traffic, packet and byte counts, and error counts enable security personnel to measure the impact of new IPS signature sets and configurations, without the need for additional monitoring tools and network taps, and without reconfiguring SPAN ports on switches.

Some bypass switches can also generate alarms (SNMP traps) when traffic on a given port exceeds a programmed use level. These traps can be used by a network management system such as IBM Tivoli or HP OpenView to alert an operator that an unusual condition exists – perhaps one in which the traffic volume could exceed the capability of the IPS.

Programmability

Some bypass switches allow you to programmatically route traffic into or around inline security tools. This feature is very helpful when troubleshooting or when upgrading the tool software.



By logging into the device from anywhere on the network, operators can monitor traffic and device status, and configure and control the device. One aspect of device control is the ability to force the bypass switch into Bypass On mode, taking the IPS offline. This capability can be handy for easily removing the IPS from service without requiring a technician to be physically on site with the IPS, saving time and travel costs.

When a bypass switch is configured in Tap mode, taking the IPS offline, the bypass assumes the function of a full-duplex network tap. In this way, it mirrors all the traffic received at network link Port A to monitor Port 1, and all the traffic received at network link Port B to monitor Port 2. This enables the IPS to continue to monitor the network traffic, acting as an out-of-band intrusion detection system (IDS), a useful way to test signature sets before actually applying them to network traffic. The device can also be used as a conventional network tap, eliminating the need to break the link to install a tap when other types of monitoring tools are required to investigate a network issue.

Modularity

Sometimes it is necessary to physically remove the IPS from the link, perhaps for maintenance, upgrade, or reconfiguring a growing network. If the IPS was deployed with an external bypass switch, the IPS can be physically removed from the link without impacting link traffic or application availability. With an internal bypass switch, or no bypass switch at all, you would have to wait for a scheduled maintenance window, perhaps get a network change authorization signed, and alert users of all applications dependent on the link that their service will be interrupted for a period. Clearly the external bypass switch saves a lot of time and trouble in this case.

But the scenario can be worse than that. So far, the examples assumed a planned event. What happens when an IPS must be taken offline or physically removed because of an unplanned situation? For example, a cable could be accidentally unplugged from the IPS during some maintenance activity.

Or the IPS could experience a physical failure such as an electrical component going bad. The external Bypass switch ensures that the application is not taken down by one of these unplanned events, should they occur.

External bypass switches eliminate the single-point-of-failure that internal bypass switches pose.

Conclusion

We've shown that an external bypass switch makes an inline security deployment more reliable and flexible as compared to depending on integrated bypass circuitry. Moreover, the cost of the external bypass switch is further justified by the value-add of improved instrumentation and the cost savings of remote management capabilities.

Customer issues:

- How do I deploy monitoring or security tools inline without adding a point of failure?
- How can I replace or upgrade my inline tools with no interruption to the business?
- How do I maximize network uptime when deploying active security solutions?

Ixia Worldwide Headquarters
26601 Agoura Rd.
Calabasas, CA 91302

(Toll Free North America)
1.877.367.4942

(Outside North America)
+1.818.871.1800
(Fax) 818.871.1805
www.ixiacom.com

Ixia European Headquarters
Ixia Technologies Europe Ltd
Clarion House, Norreys Drive
Maidenhead SL6 4FL
United Kingdom

Sales +44 1628 408750
(Fax) +44 1628 639916

Ixia Asia Pacific Headquarters
101 Thomson Road,
#29-04/05 United Square,
Singapore 307591

Sales +65.6332.0125
Fax +65.6332.0127

915-6688-01 Rev. B, December 2015