Improve Network Reliability With External Bypass Switches

## DEPLOYMENT SCENARIO: INLINE VISIBILITY ARCHITECTURE

The goal of any IT team is to deliver network and application services with maximum quality of experience, including availability and uptime. One way to accomplish this goal is to add external bypass switches in front of inline security and monitoring tools. While directly deploying inline security tools can create an improved line of defense, these tools can also result in single points of failure, should they falter. An internal bypass within the tool can minimize this risk but it creates another point of service interruption, should the device need to be removed at a later date.

An external bypass switch eliminates the pain of direct deployments of inline tools because it provides both automatic and on-demand fail-over capabilities with a barely perceptible impact (milliseconds) to the network. Since the switch always stays in the network, it can be placed into bypass mode as needed so that security and monitoring devices can be added, removed, or upgraded as necessary.

This solution provides a methodology that creates failsafe deployments of inline security and monitoring tools to ensure high availability, maximum uptime, and the maximum mean time between failure (MTBF) for network components.

SOLUTION COMPONENTS:

- Bypass Switch
- Inline security & monitoring tools
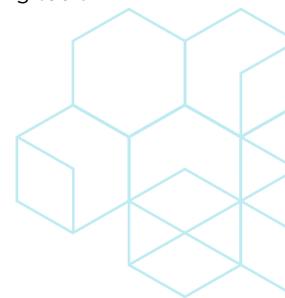
IXIA

A Keysight Business

BENEFITS

- Eliminate single points of failures for inline device deployments
- Eliminate downtime due to tool upgrades/removal
- Reduce network risk with bypass solutions that have higher MTBFs
- Create flexibility to add/remove inline security tools without network impacts

SOLUTION OVERVIEW

This network visibility solution allows you to:

- Remove single points of failure by adding fail-over capability to inline tools
- Increase network MTBF by deploying an external bypass switch which has a 5 times better MTBF over integrated bypass solutions
- Eliminate down time while replacing or upgrading devices by using external bypasses that allow you to add/remove tools at will

THE VALUE OF AN EXTERNAL BYPASS SWITCH

An external bypass switch allows failsafe deployments of inline security and monitoring tools to ensure high availability and maximum uptime. Even a strong mix of security and analytics tools can lead to network reliability risks as regular rebooting, maintenance, and upgrades of those devices will increase the chances of a costly network outage. In the event that an inline tool becomes unavailable, it can completely bring down the network link, significantly compromising network uptime and disrupting business continuity. According to Ixia conducted research, this can be a significant problem for the almost 20% of IT enterprises that directly deploy inline security tools and the 40% of enterprises that deploy internal bypass solutions instead of external-based solutions. The bypass switch eliminates the pain of direct deployments of inline tools and the complications of internal bypass functionality.

Bypass switches fit into the existing networking ecosystem; allowing the existing network to function as currently designed without forcing changes to accommodate network visibility components. These bypass switches give you more flexibility to add/remove inline security tools without network impact. When the fail-open bypass function is activated, all traffic can continue downstream. The failover time is typically less than 10 milliseconds. If you prefer a fail-closed option (where no traffic continues in or out of the network), that is available as well.

> Even a strong mix of security and analytics tools can lead to network reliability risks as regular rebooting, maintenance, and upgrades of those devices will increase the chances of a costly network outage.

Figure 1 Bypass switches deployed in front of security and monitoring tools
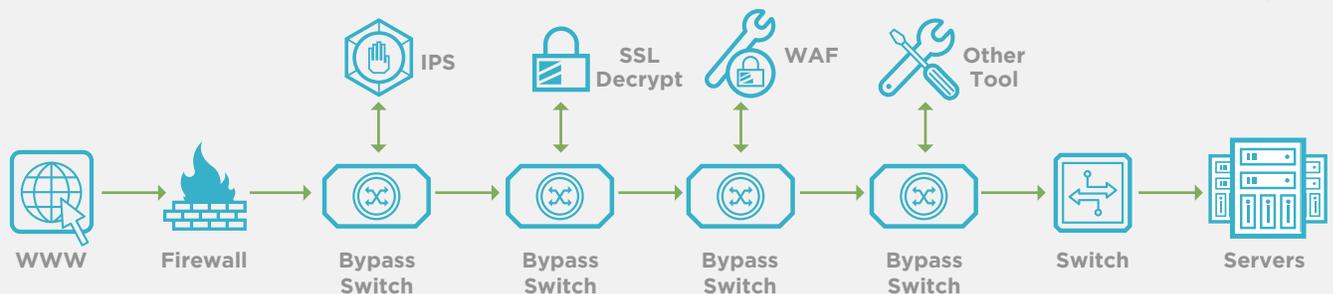
Typical network failures are indicated by Link Fault Detection (LFD) that may require human intervention to initiate fail-over. However, a self-healing architecture using Heartbeat messages (that are passed back and forth between the bypass switch, network packet brokers (NPBs), and security tools) can be used to initiate faster fail-overs that increase network availability over other solutions.

The stand-alone (external) bypass offers superior protection to direct security tool deployments and integrated bypass options. External bypass switches have been shown to have a reliability that is 5 times better than internal bypass functions. The MTBF for an external bypass is approximately 450,000 hours versus an integrated bypass with an MTBF of 80,000 hours. In addition, when you replace a security tool, the integrated bypass may have to be removed as well, destroying any supposed bypass advantage. The external bypass solution eliminates this issue.

SUMMARY

External bypass switches are an important component for increasing the reliability and availability of data networks. Their simplicity makes them easy to deploy while their advanced feature set delivers unsurpassed availability. These devices provide an effective and powerful line of defense that reduces the risk of inline security and monitoring tool deployments. This is especially true when the MTBF for an external bypass solution is 5 times better than other bypass solutions on the market.

VISIBILITY ARCHITECTURE SOLUTIONS FROM IXIA

Ixia's network visibility solutions provide high value while eliminating network blind spots and data acquisition issues. Learn more about Ixia's Bypass Switch and Network Packet Broker technology.

IXIA WORLDWIDE

26601 W. Agoura Road
Calabasas, CA 91302

(Toll Free North America)
1.877.367.4942

(Outside North America)
+1.818.871.1800

(Fax) 1.818.871.1805

www.ixiacom.com

IXIA EUROPE

Clarion House, Norreys Drive
Maidenhead SL64FL
United Kingdom

Sales +44.1628.408750
(Fax) +44.1628.639916

IXIA ASIA PACIFIC

101 Thomson Road,
#29-04/05 United Square,
Singapore 307591

Sales +65.6332.0125
(Fax) +65.6332.0127