WHITE PAPER

The Surprising Ways that Inline Bypass Helps Protect Network Operations

Introduction

Your organization depends on all kinds of inline tools to keep your network up and running, but those same tools can fail, leaving you vulnerable. Moreover, as network speeds increase, slower tools can bottleneck network traffic, making organizations purchase more and more tools, which then introduce complexity and cost. There is a better way to increase network resiliency while reducing security issues, and that's inline bypass.

Inline Tools Are Important But Can Be Problematic

Inline tools are powerful weapons for securing and monitoring the network. However, their greatest asset – the ability to be inline with the production network – is also their greatest liability. That's because deploying and optimizing these tools presents several challenges:

1. Inability to Keep Up with the Speed of Networking
First, many inline tools are unable to handle higher rates of traffic when networks upgrade – for example, from 10Gb to 40Gb. As traffic arrives more quickly, the tools do not have enough time or capacity to process it all. They can become bottlenecks when network traffic peaks, causing unacceptable slowing of application performance. That's one way inline tools can become single points of failure.

2. Loss of Functionality due to Power Outage or Other Causes
Critical applications can stop in their tracks when one of these tools loses power, has a software failure or is taken offline for maintenance, nullifying the investment and business benefit of high-speed networks.

If you do nothing, you will have to put up with lower performance of tools to do their jobs and possibly decreased performance of your network. In response, many organizations upgrade their infrastructure, which can be difficult as well as costly. Remedying this situation is not as easy as having the budget, because inserting, upgrading or changing tools requires complex coordination of maintenance windows between NetOps and SecOps.

But there is an alternative approach that is more cost-effective, easier to manage and more responsive to the needs of the business.

The use of a next-generation network packet broker and its inline bypass functionality can minimize these challenges. In fact, inline bypass can:

- Optimize tool performance and maximize security
- Balance network performance and security
- Maintain network traffic continuity
- Help you test and deploy new tools

Let's take a closer look.

What Is Inline Bypass?

Let's face it: most non-technical executives and managers prioritize business processes over perfect network operations. They are unhappy when applications or the network slow down or become unavailable, and are not receptive to excuses related to difficulties with inline tools. Having said that, most businesses will also prioritize network uptime over security, so that when an inline inspection tool fails, it is preferable to allow traffic to continue uninspected than to cause a disruption in service.

Fortunately, the inline bypass feature of a next-generation network packet broker (NGNPB) can keep application traffic flowing when an inline tool fails because of a power outage or a software or hardware failure.

The NGNPB monitors the health and performance of the tool with bidirectional heartbeat packets. If the tool goes offline or is overwhelmed by spikes in network traffic, the NGNPB arranges for the network traffic to bypass it. When the tool comes back online, the NGNPB automatically restarts traffic through it. In this way, inline bypass removes any failure points by automatically switching traffic via bypass mode – keeping critical network traffic and protection up and running.

Here are some of the other surprising ways that inline bypass protects business operations; if you are evaluating solutions, it would be wise to keep these in mind:

1. Optimizing Tool Performance and Maximizing Security
Inline bypass maximizes the efficacy of inline tools without compromising network availability by enabling operational staff to select and distribute specific traffic of interest across multiple tools. This means that network security scales linearly with the

number of tools deployed while also helping to ensure that a given tool can see all traffic that corresponds to specific user and server sessions. This type of targeted traffic forwarding is vital to detecting advanced persistent threats (APTs) more quickly. The net effect? Security tools now inspect the most relevant traffic and increase the probability of uncovering and responding to risks faster.

Unlike the traditional active-standby arrangement where a standby inline tool is completely unutilized until the active tool fails, inline bypass provides the option to send traffic to a backup tool in a 1+1 or N+1 protection scheme. In the latter case, traffic can be distributed across multiple inline tools simultaneously – for example, all three Advanced Threat Prevention (ATP) appliances could be used in an inline tool group instead of using them in a "2 active ATP + 1 standby ATP" appliance mode where the standby ATP appliance is unused most of the time. Such a model ensures that all assets in the inline security prevention stack are utilized to maximum potential and that organizations get the most out of their existing tool investments.

In this way, inline bypass is employed to share the load across multiple inline devices so that you can scale security monitoring to the speed of networking. This helps ensure that no single device becomes a bottleneck that slows network traffic. The load sharing guarantees that devices monitor complete sessions, including both inbound and outbound traffic.

The bottom line is that with inline bypass, you can keep up with growing network traffic volumes scale by controlling which traffic goes to which tools and maximize network availability, even with failing tools or tools that are offline due to power outages, software and hardware failures, maintenance and replacement.

2. Balancing Network Performance and Security

Being able to select in which modes your tools operate gives you the ability to make intelligent trade-offs between performance and security, for example using devices in detection mode out of band, but switching them into inline protection mode when an attack is detected, so they can block malicious network traffic immediately.

NGNPBs provide a common platform to deliver traffic feeds to out-of-band security and analytics tools that only need to scan a copy of the traffic, and to inline tools that can block malicious traffic as soon as it is discovered. NGNPBs offer benefits in both cases, plus the ability to be switched back and forth automatically, in milliseconds, between out-of-band and inline modes. This allows organizations to deploy some inline tools such as an Intrusion Prevention System (IPS) and APT systems in an out-of-band, "detect only" mode so they have no impact on network latency, but have them automatically switch over to inline mode immediately when an attack is detected. Until the threat is resolved, the tool can block malware, links to compromised websites and hacker communication traffic. This arrangement maximizes application performance and availability under normal conditions, but dynamically changes priorities in favor of security when needed.

3. Maintaining Network Traffic Continuity

Bypass protection comes in two varieties: logical and physical. Both operate on the principle that traffic continuity must be maintained continuously even if the traffic cannot be inspected due to a power outage.

A physical bypass switch provides users with the ability to physically forward packets in the event of an NGNPB power failure. It also allows you to perform maintenance and upgrade your tools without impacting network operation or downtime. Switching to protected mode should occur automatically and without software intervention upon the loss of power.

With logical bypass, the NGNPB constantly gauges the health of inline tools using bi-directional heartbeat packets. Whether the tool fails because it loses power or stops forwarding traffic, the NGNPB can bypass the failing tool and maintain network uptime. Alternatively, such as when a tool fails to block known bad traffic, the NGNPB can trigger a network failover to a redundant path that is protected by healthy tools.

4. Testing and Deploying New Tools

The inline bypass feature of NGNPBs also makes it easier to test and deploy new security and analytics tools. Tools being evaluated can be fed real production traffic in out-of-band mode, which increases the accuracy of the testing. Because an NGNPB can switch devices from out of band to inline in seconds, it is easy to test new tools with real network traffic. You can validate existing tools after upgrades in detection mode, test alternative new tools side-by-side with the same data, and "train" tools that need to monitor the network and establish baseline normal behaviors. When you are ready, it only takes a moment to switch the tool to inline mode and no rewiring is required.

Inline Bypass Benefits Overview

Because inline bypass filters and distributes just the relevant network data to inline tools, NGNPBs enable a resilient, simplified security architecture at a significantly reduced cost. In fact, with a NGNPB, you can:

- Simplify architecture and enable tools to do more, with faster onboarding of patches and new technology, leading to a 50% reduction in the cost of security efforts and a 153% ROI[1]
- Roll out and test new security tools in minutes instead of weeks or months

[1] Shaheen Parks, "The Total Economic Impact™ Of Gigamon - Cost Savings And Business Benefits Enabled By Gigamon," Forrester Research, April 2016. https://www.gigamon.com/content/dam/gated/ar-forrester-economic-impact-of-gigamon.pdf

- Lower CapEx by increasing the efficiency of tools, inspecting more traffic with fewer tools
- Lower OpEx by reducing planned and unplanned network outages
- Get access to and control of data for improved visibility everywhere for:
  - Faster roll-out of security and monitoring initiatives
  - Improved utilization of tools
  - Holistic security architecture
- Improve confidence in security posture:
  - Enables deeper and wider inspection of network traffic
  - Gives you faster roll out of new tools
  - Gives you security at speed of network
  - Makes it easier to meet compliance requirements
  - Simplifies new technology adoption

How Gigamon Can Help

The Gigamon Visibility Platform, a next-generation network packet broker purpose-built for tools to work more efficiently across physical, virtual and cloud environments, offers an inline bypass switch, which enables enterprises to:

- Keep up with growing network traffic volumes by improving the performance of inline tools
- Streamline operations so you can complete new and ongoing functions in hours versus weeks
- Eliminate single points of tool failure by creating a resiliency layer

The Gigamon Visibility Platform monitors the health and performance of the tool with bidirectional heartbeat packets. If the tool goes offline, or is overwhelmed by spikes in network traffic, it can be bypassed in milliseconds, keeping critical application traffic up and running.

The Gigamon Visibility Platform cannot become a single point of failure either. Redundant components reduce the risk of issues, and physical relays send traffic through in “fail to wire” mode in the event of a power loss.

For organizations unable to keep up with increasing network speeds, volumes of data and potential cyber threats, Gigamon inline bypass delivers relevant network data to downstream inline tools at the rate they can consume. Unlike standalone tools, our solution is purpose-built to reduce architectural complexity, stop tool sprawl and contain costs.

Gigamon inline bypass simultaneously maximizes tool performance, network resiliency and operational efficiency. It optimizes the performance of tools by delivering just the traffic that they are designed to inspect and distributing traffic across multiple tools. The integrated physical and logical bypass functions deliver the highest resiliency that consequently allows simple insertion and removal of inline tools for upgrade and replacement or testing of new tools without impacting availability.

Summary

We’ve seen how inline tools can fail, either due to a power outage, software or hardware issues, or because they are overwhelmed by faster network speeds. The solution to these challenges is inline bypass, an important part of a next-generation network packet broker. If the tool goes offline, or is overwhelmed by spikes in network traffic, The Gigamon Visibility Platform can bypass the tool in milliseconds, keeping critical application traffic up and running.

About Gigamon

Gigamon is the recognized leader in network visibility solutions, delivering the powerful insights needed to see, secure and empower enterprise networks. Our solutions accelerate threat detection and incident response while empowering customers to maximize their infrastructure performance across physical, virtual and cloud networks. Since 2004 we have cultivated a global customer base which includes leading service providers, government agencies as well as enterprise NetOps and SecOps teams from more than 80 percent of the Fortune 100.

For the full story on how we can help reduce risk, complexity and cost to meet your business needs, visit www.gigamon.com.

Gigamon®

Worldwide Headquarters
3300 Olcott Street, Santa Clara, CA 95054 USA
+1 (408) 831-4000 | www.gigamon.com