Feature Brief

Why Security Tools Need Inline Bypass

Security at the speed of your network.

Inline Bypass: Increase application resiliency and get the most out of your security tools.

Key Benefits

- ✓ Prevent inline security tools from becoming points of failure that disrupt applications.
- ✓ Get the most from your security tools.
- ✓ Improve ROI with increased efficiency and scale.
- ✓ Update or replace security tools without interrupting applications or network uptime.
- ✓ When attacked, shift tools from detection mode to inline prevention mode in seconds.
- ✓ Test and compare new security tools with production network traffic.
- ✓ Keep network traffic flowing in the event of a power loss with fail-to-wire physical bypass protection.

Optimize Resiliency, Performance, Security and Cost

Inline security tools — Web Application Firewalls (WAFs), Intrusion Prevention Systems (IPS) and Advanced Threat Protection (ATP) — are vital for securing your network, but can create their own problems, such as:

- They represent network points of failure.
- When an inline tool loses power, has a software failure or is taken off line for maintenance, critical applications can be stopped in their tracks.
- When network traffic peaks and security is most critical, inline tools can become bottlenecks that degrade application performance.

Fortunately, there's an easily deployed, cost-effective solution: The Inline Bypass feature found in the GigaSECURE® Security Delivery Platform (GigaSECURE), the next-generation network packet broker purpose-built for security. Without much effort, Inline Bypass lets you:

- Prevent inline security tools from becoming single points of failure.
- Efficiently distribute network traffic across security devices, helping you avoid the high costs from purchasing large systems for every network link.

You can also make intelligent trade-offs between network performance and security, such as:

- Choosing to inspect high-risk traffic while bypassing traffic for which lower latency is critical.
- Deploying security tools in out-of-band detection mode so they don't affect network latency, but then, when an attack is detected, easily switching them into inline protection mode to block malicious activity in real time.

Keep Traffic Up and Running

Security tools sometimes go offline because of power outages, software and hardware failures, maintenance and replacement. GigaSECURE monitors your tools' health and performance with bidirectional heartbeat packets. Then, when a tool does go offline or is overwhelmed by spikes in network traffic, GigaSECURE can bypass the tool and keep critical application traffic up and running.

Benefit from Next-Gen Capabilities

Your inline security tools' limited traffic capacities may fall below the bandwidth of the network traffic that needs inspection. Furthermore, as networks evolve from 10Gb to 40Gb and 100Gb, deploying tools with matching high-speed interfaces may break limited budgets.

Here too GigaSECURE has you covered by distributing inline traffic across your security tools. Not only does distribution increase your overall inspection capacity, but it also scales older, lower-speed tools to secure higher-speed networks, improving your ROI.

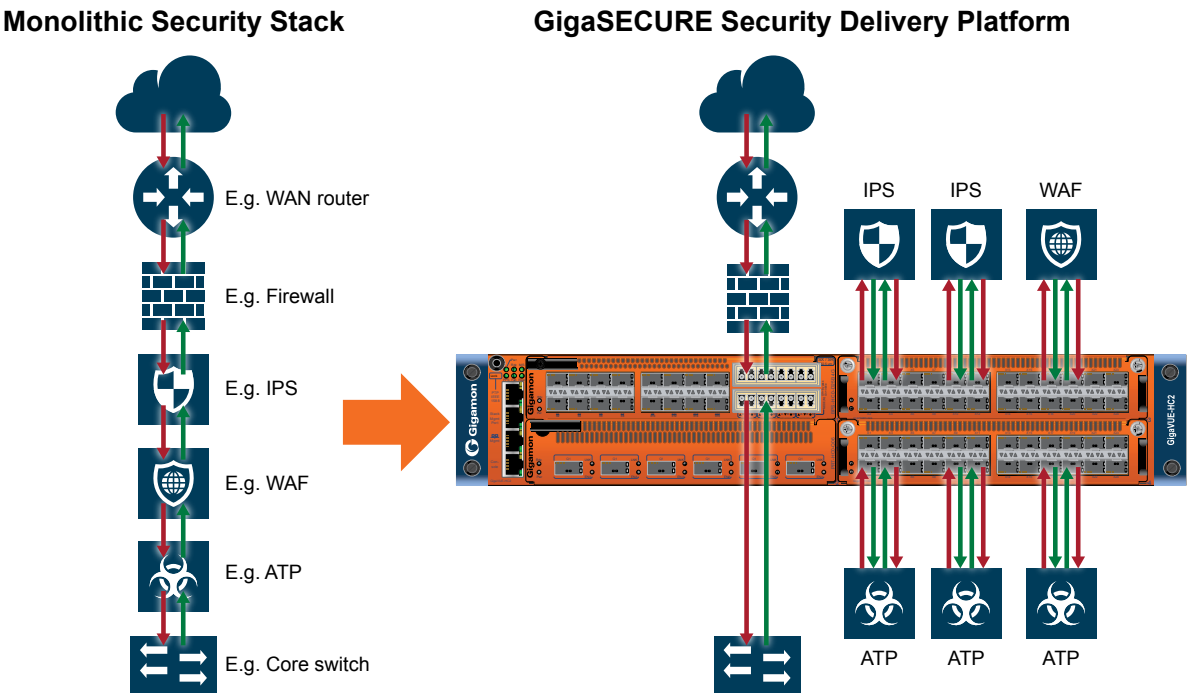

Figure 1: Scaling threat prevention tools with GigaSECURE

How does it work? The traffic distribution algorithm operates at line rate in hardware and lets each tool see complete, bidirectional sessions for the greatest effectiveness. This capability also has built-in resiliency; when tools fail or go offline, the system redistributes traffic to the remaining healthy tools. Adding 1+1 or N+1 redundancy provides even greater security and network availability.

Migrate Security Tools Between Detection and Prevention Modes

GigaSECURE supports both out-of-band and inline security tools, which lets you replicate inline traffic to out-of-band detection tools for both security and network performance monitoring. From this traffic GigaSECURE can also generate metadata and then send it to SIEMs (Security Information and Event Management) and other tools that consume IPFIX or CEF-based data.

Most inline prevention tools can also operate in an out-of-band detection mode. You can use the GigaSECURE Security Delivery Platform to deploy the tool inline even though it is in detection mode by sending a copy of the inline traffic. When you are ready to move the tool inline, a flip of the proverbial switch will send it traffic directly. Another flip can bring it back to detection mode.

In performance-sensitive application environments, it often makes sense to run security tools out of band in detection mode, so they have no impact on network latency. Until the threat is resolved, the tool can block malware, links to compromised websites and command-and-control traffic.

Easily Update, Deploy and Test Security Tools

With the GigaSECURE Inline Bypass feature you can also take tools off line for updates or replacement without scheduling maintenance windows or interrupting access to applications.

Also, because GigaSECURE can switch devices from out of band to inline in seconds, you'll find it easy to test security tools with real network traffic. Examples include:

- Validating upgraded tools in detection mode.
- Training tools that need to monitor the network by establishing baseline normal behaviors.

Then when you are ready, it only takes a moment to switch the tool back to inline mode.

Learn More About GigaSECURE Inline Bypass

To see how your network will benefit from the Inline Bypass feature of the GigaSECURE Security Delivery Platform, please visit **www.gigamon.com/gigasecure**.

6116-01 04/18

Gigamon®

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