Whitepaper

Inline Bypass: Scaling Inline Threat Prevention Tools to Keep Pace with High-Speed Networks

Are your threat prevention tools struggling to keep up with the increasing speed of your organization's network? Is the number and variety of security tools you think you need starting to tax your budget and overcomplicate your security infrastructure?

This paper outlines how the GigaSECURE® Security Delivery Platform inline bypass functionality helps facilitate the rollout of security initiatives by enabling inline threat prevention tools to scale and keep pace with high-speed networks. With the GigaSECURE Security Delivery Platform, businesses can cost-effectively improve their security posture without sacrificing network performance.

The Disruption-Defense Conundrum

In today's fast-paced markets, businesses depend upon high-speed networks to boost collaboration, improve innovation and increase productivity. Unfortunately, increasing network data rates and consequent network upgrades have major repercussions for security administrators, especially those who rely on best-of-breed inline threat prevention tools. These tools simply can't keep pace with faster networks. As traffic arrives more quickly, the tools do not have enough time or capacity to process it all. As a result, the risk of attack rises, which in turn, can nullify the investment and business benefit of high-speed networks.

Not All Traffic Is Created Equal – or at Least, Need Not Be Equally Inspected

In many cases, inline security tools are unable to handle higher rates of traffic because of a network upgrade – for example, from 10Gb to 40Gb – and organizations are forced to upgrade their security infrastructure, which is difficult, if not architecturally impossible or economically impractical.

An alternative to a complete and expensive upgrade is to increase the effectiveness of existing tools by sending them only relevant data to process. All security tools do not need to inspect all traffic. For example, a web application firewall (WAF) only needs to inspect web traffic, an intrusion prevention system (IPS) may not need to re-inspect traffic that has already been inspected in another zone and an advanced persistent threat (ATP) system may not need to inspect traffic coming from an internal zone or a specific traffic category that is reasonably secure.

In other words, different traffic should be handled in different ways. Briefly put, it's about delivering the right traffic to the right security tool at the right time. If a security tool only receives the precise network data it needs to inspect – instead of being overloaded with irrelevant data – it can keep up with growing data volumes and start to detect and prevent more threats.

Inline Bypass in the GigaSECURE Security Delivery Platform: Increase Security without Compromising Network Availability

The GigaSECURE Security Delivery Platform is a next-generation network packet broker that has been purpose-built for security. An integral component of the solution is a set of capabilities called "inline bypass," which is designed to maximize the efficacy of inline threat prevention tools without compromising network availability by enabling operational staff to select and distribute specific traffic of interest across multiple inline security tools.

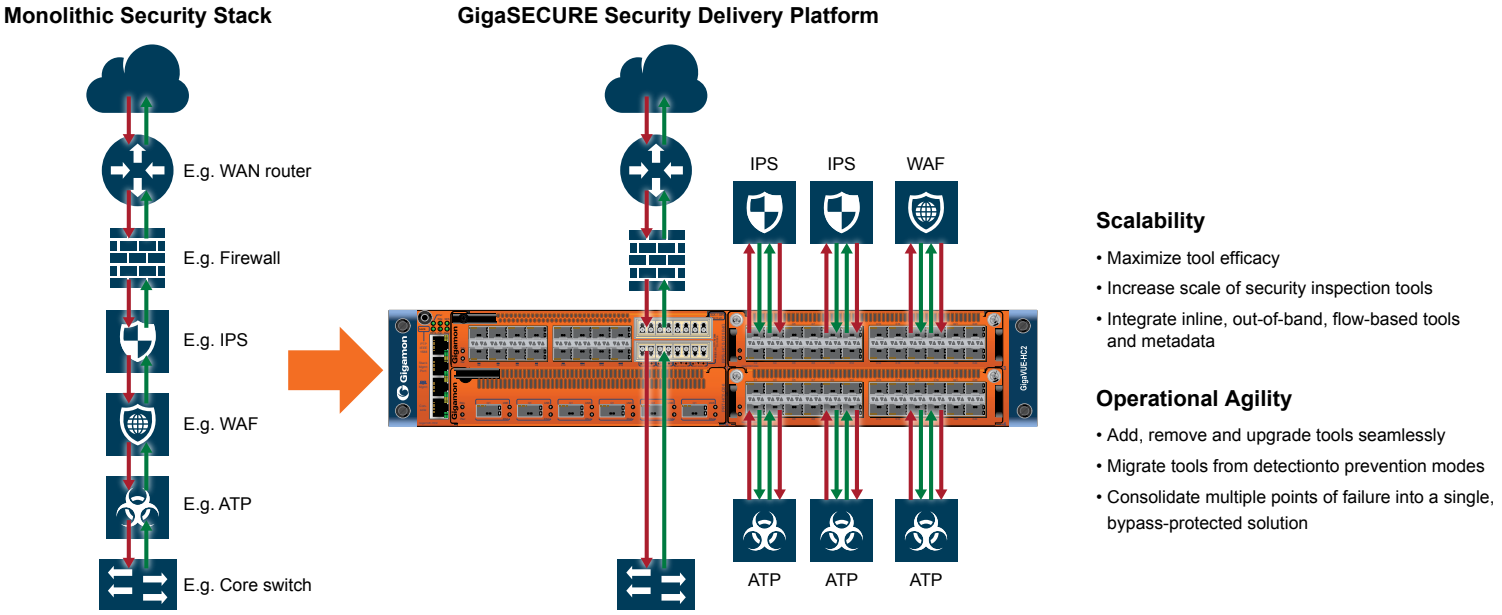

Figure 1: Scaling Threat Prevention Tools with GigaSECURE®

0002-01-ND-GS-ITP-HC2-IL

Integrated Physical and Logical Bypass Protection

By offering integrated physical bypass protection, the GigaSECURE Security Delivery Platform itself cannot become a single point of failure. While its redundant, load-sharing power supplies make it unlikely, the GigaSECURE Security Delivery Platform can engage relays in fail-to-wire mode to keep the network up and running even in the event of a power loss. Further, packets and flows are not processed in software and therefore, is not susceptible to the styles of processing overloads that are common with security tools. What's more, its ability to make packet-forwarding decisions in silicon helps ensure that it adds no material delay to network traffic.

Much like a GPS navigation system can provide real-time traffic updates and suggest alternative routes around congested areas, bypass protection can detect the failure of an active tool and redirect traffic to a standby tool. The GigaSECURE Security Delivery Platform constantly gauges the health of inline tools using bi-directional heartbeat packets. If an inline security tool fails, configuration options allow either the failed network link or the security tool to be bypassed to maximize availability.

Unlike the traditional active-standby arrangement where a standby inline security 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 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 helps ensure that all assets in the inline security prevention stack are utilized to maximum potential and that organizations get the most out of their existing security tool investments.

In the event of an inline security tool failure, the GigaSECURE Security Delivery Platform detects the failure and redistributes traffic among the remaining healthy tools in that tool group. Once the failed tool comes back online – a fact discerned by measuring the re-emergence of heartbeat packets – the GigaSECURE Security Delivery Platform can again, begin forwarding traffic to the recovered tool for inspection. Heartbeat settings to react to outages in less than 50 milliseconds or tune the heartbeat timeout to bypass any tools that are overloaded and adding excessive latency.

In contrast to the monolithic security stack, shown to the left in Figure 1 the GigaSECURE Security Delivery Platform, to the right, provides an insulation layer that shields the network and security tools from changes in one another. Further, this approach allows NetOps to maintain control over one set of infrastructure elements – for example, WAN router, firewall and core switch – and SecOps to separately handle upgrades, maintenance, additions or removals of inline security tools – for example, IPS, WAF, ATP – without compromising network uptime.

Maximize Security Tool Efficiency

Ideally suited to address the network-data-rate-to-security-appliance-throughput disparity, the GigaSECURE Security Delivery Platform can distribute the load across multiple security tools such that network security scales linearly with the number of tools deployed while also ensuring that a given security tool can see all traffic that corresponds to specific user and server sessions.

This type of targeted traffic forwarding is vital to detecting APTs more quickly. Rather than monitor all traffic flowing over the network, the GigaSECURE Security Delivery Platform can use Flow Mapping® technology to selectively forward specific sessions for monitoring and bypass the rest, with filtering criteria based on application type, like database, web or email; TCP/UDP port; IP and MAC address of servers and endpoints; or any combination. Not only is this a practical compromise between performance and security, but it negates the need to unnecessarily purchase more or higher capacity security tools. Organizations can dynamically apply these configurations using the APIs exposed by the GigaSECURE Security Delivery Platform and integrate them into a modern DevSecOps security environment.

The net effect? Security tools now inspect the most relevant traffic and increase the probability of uncovering and responding to risks faster.

Consolidate and Optimize Security Monitoring

While sophisticated cyberthreats may merit having security devices on every segment and at every location, it is often cost-prohibitive to place firewalls, anti-malware and content-inspection devices on every network segment or every internet gateway exit point. It is far more efficient and less expensive to aggregate network traffic from multiple network segments into the GigaSECURE Security Delivery Platform and send the aggregated traffic of interest to a centralized, higher-capacity security tool for inspection. Organizations can also apply a similar approach to remote offices, especially if they are backhauling all traffic from those remote offices to a few aggregation points. This centralized approach helps ensure that they get the most from their large-scale security computing investments at aggregation points like data centers and campuses.

The GigaSECURE Security Delivery Platform can aggregate and forward traffic streams from multiple network segments and send traffic of interest to a common security tool. The GigaSECURE Security Delivery Platform tags traffic so that forward and return traffic is sent to the correct segment. This capability is also useful in network architectures that feature asymmetric routing.

In networks with redundant paths, the GigaSECURE Security Delivery Platform can monitor both active and standby network links, eliminating the need to replicate the entire security stack for each link. By preserving the session integrity regardless of the path it takes, security devices receive whole sessions of bidirectional traffic.

Since most security architectures are multi-vendor, best-of-breed stacks of specialized products, their need to inspect the same traffic may conflict and burden the network. The GigaSECURE Security Delivery Platform addresses this issue by aggregating the traffic forwarding and distribution function and infusing it with intelligence that not only resolves packet contention, but also enables security tool optimization. For example, the GigaSECURE Security Delivery Platform will only send email traffic to the email inspection tool; only web traffic to a WAF; and all traffic, if desired, to a group of IPS. Consolidating traffic-forwarding policies in this way facilitates scaling of the security stack to accommodate new technologies and proof-of-concept deployments – without network disruption. Moreover, any additional tools that require access to network traffic simply connect to the GigaSECURE Security Delivery Platform to receive the necessary visibility.

Seamlessly Add, Remove and Upgrade Security Tools

With the GigaSECURE Security Delivery Platform, SecOps can apply software patches and perform upgrades without lengthy coordination of maintenance windows, network downtime or reduced security. Instead of being connected directly inline, security tools are connected to the GigaSECURE Security Delivery Platform, where they can be easily removed, rebooted or updated without affecting the network. Before the inline tool is taken out of service, the GigaSECURE Security Delivery Platform can bypass traffic to that tool until it is once again, ready to begin inspection.

When deploying multiple inline tools, SecOps can upgrade them sequentially without having a large maintenance window or extended network outage and even better, add tools to the GigaSECURE Security Delivery Platform with no need for a maintenance window. Traffic can be directed to a new tool with a software command and minimal impact to the network.

Migrate Security Tools Between Prevention and Detection Modes

Many inline security solutions can also operate in an out-of-band mode. In fact, some security devices have "learning modes" where they spend days or weeks passively monitoring the network to baseline normal behavior to flag anomalies later. While out of band, the security appliance will receive only a copy of the traffic. Once tuned and ready to operate in an inline configuration, it can be programmatically moved by the GigaSECURE Security Delivery Platform without any rewiring.

The ability of the GigaSECURE Security Delivery Platform to move a security tool between prevention and monitoring – or detection – modes is a powerful capability that security administrators can use in multiple ways. For example, they can:

- Validate the operation of a prevention tool in detection mode after it has been upgraded with a new software.
- Deploy threat prevention tools in threat detection mode in latency-sensitive application environments or those where the network data rate-security impedance mismatch is very high – for example, for service providers or in 40Gb/100Gb networks running 1Gb/10Gb security tools. When a tool detects a threat, the GigaSECURE Security Delivery Platform can be programmed to rapidly move the inline tool to prevention mode. Such an approach ensures that latency is minimized when no malicious threat is detected and that higher latencies are only seen when the inline tool is actively blocking malicious flows.

Integrate Inline, Out-of-Band, Flow-Based Tools and Metadata

To further augment the effectiveness of an organization's stack, a security administrator can leverage the GigaSECURE Security Delivery Platform to simultaneously deliver traffic of interest to both inline and out-of-band tools. It can also be used to generated flow data – for example, NetFlow or IPFIX – to flow-based tools and feed metadata to other out-of-band security tools, such as security information and event management (SIEM), user and entity behavior analytics (UEBA), security analytics. By leveraging the GigaSECURE Security Delivery Platform to tap into virtual and cloud infrastructures, an organization can significantly expand the coverage of its security stack in a very cost-efficient manner. Similarly, non-security application performance monitoring (APM) and network performance monitoring (NPM) tools can receive network traffic from the same GigaSECURE Security Delivery Platform, thereby enabling multiple teams in an organization to benefit from the investment.

Moreover, the GigaSECURE Security Delivery Platform can also offload compute-intensive SSL decryption from inline tools; it simply decrypts traffic once and distributes it to any number of inline or out-of-band tools that require it. With this approach, organizations can realize significant ROI, efficiency and performance benefits.

Summary

As network data rates continue to grow, security architects and administrators need an architecture that enables their threat prevention stacks to efficiently keep pace without compromising network resiliency. The integrated physical and logical inline bypass capability is a key component of the GigaSECURE Security Delivery Platform that enables security administrators to simultaneously maximize threat prevention, security resilience and network uptime. Using this approach, security architects can stop tool sprawl, cut tool costs and significantly shorten the time required to roll out threat prevention initiatives in their organization.

3260-01 02/18

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