Feature Brief

为什么安全工具需要采用Inline Bypass智能引流方案?

实现安全与网络同步发展

Inline Bypass：提升应用弹性，发挥安全工具的最大潜力

主要优势

- ✓ 防止串接安全工具出现单点故障，影响应用性能
- ✓ 最大限度发挥安全工具的优势
- ✓ 提升效率、扩大规模，实现更高投资回报率
- ✓ 在不影响应用和网络运行的情况下对安全工具进行更新或替换
- ✓ 一旦有攻击发生，可在数秒内由检测模式切换至串接防御模式
- ✓ 使用生产网络流量来测试和比较全新安全工具
- ✓ 在发生断电且无法启动物理旁路保护的情况下，确保网络流量正常传输

实现弹性、性能、安全及成本优化

串接安全工具 – Web应用防火墙(WAF)、入侵防御系统(IPS)、高级威胁防护(ATP)，对于网络安全异常重要，但同时也会带来一定的问题，例如

- 有可能发生网络单点故障
- 当串接工具出现断电、软件故障，或者需要关机维护时，会导致关键应用中断；
- 网络流量达到峰值时，安全至关重要，但是启用安全工具却有可能会变为性能瓶颈，导致应用性能下降。

令人欣慰的是，Gigamon有一套易于部署且具成本优势的解决方案：GigaSECURE® SDP安全交付平台，该平台所具有的Inline Bypass智能引流功能，专为网络安全而打造。

无需耗费太多精力，Inline Bypass智能引流方案，可助您实现：

- 防止串接安全工具成为单点故障隐患
- 可将多链路的网络流量分发至安全设备，节省了单独为每个网络链路购置多套安全系统的高额费用

此外，您还可在网络性能与安全之间实现智能平衡，比如，

- 抽查高风险流量，同时对那些要求低延迟的流量进行旁路引流
- 以带外检测模式部署安全工具，这种方式不影响网络延迟，同时在检测到攻击时，可轻松切换至串接防护模式，对恶意行为进行实时阻截

确保流量正常传输

由于受到断电事故、软硬件故障，或者维修保养、设备替换等因素影响，安全工具会出现掉线状况。GigaSECURE可利用双向心跳数据包来监测工具运行状况和性能表现。一旦有工具掉线或者因为网络流量波峰而出现性能过载，GigaSECURE 可实现工具旁路，确保关键应用流量正常传输和运行。

下一代解决方案的功能优势

有些串接安全工具的流量处理能力非常有限，无法满足网络流量检测所需的带宽要求。同时，随着网络从10Gb向40Gb甚至100Gb演进，部署具备相应高速接口的安全工具所耗费成本可能会超出用户有限的预算。

GigaSECURE将串接流量分发至安全工具，借此来保护客户安全；流量分发这一方式不仅能够加强网络整体检测能力，还可实现利旧低速工具的功能扩展，获得更高速网络，从而提升投资回报率。

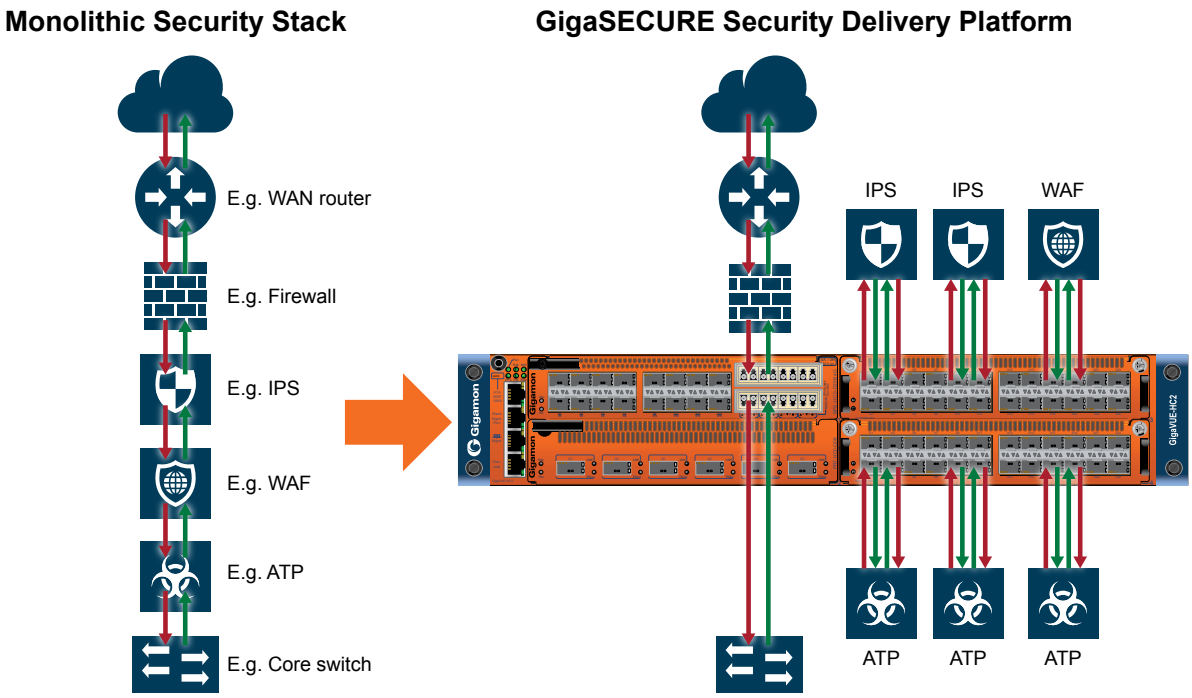

Figure 1: Scaling threat prevention tools with GigaSECURE

GigaSECURE是如何工作的呢? 流量分发算法以硬件线速运行，并在所有工具之间建立完整双向会话。此外，它还具备内置弹性；当某些安全工具出现故障或掉线的情况，系统会将流量重新分发至其他正常运行的安全工具。这种全新的1+1或 N+1冗余设计可提供更高的安全性和网络可用性。

让安全工具在检测模式与防御模式之间灵活切换

GigaSECURE支持带外和串接安全工具，让您能够将网络流量复制至带外检测工具以实现对安全和网络性能的监测。此外，该流量还可支持GigaSECURE生成Metadata元数据，并进一步将数据资料分发至安全信息和事件管理平台(SIEM)及可处理基于IPFIX或CEF数据的其他工具。

大多数串接防御工具亦可在带外检测模式下运行。即使处于检测模式，您也可以通过复制串接流量的方式使用GigaSECURE SDP安全交付平台来部署串接工具。若您准备将工具转至串接模式，只需点击一个普通开关即可向其直接发送流量；同理，您也只需点击一下开关便可将其切换回检测模式。对于那些对性能敏感的应用环境来说，能够在带外检测模式下运行安全工具通常具有重大意义，因为它们不会对网络延迟带来任何影响。 在威胁确定被处理之前，安全工具将持续阻截恶意软件、阻断对受攻击网站的访问、阻止访问命令与控制(C&C)服务器的流量。

实现安全工具的轻松更新、部署和测试

借助GigaSECURE Inline Bypass智能引流功能，您无需特意安排维护空窗期或者中断对应用的接入，便可随时让工具停机以进行更新或替换等操作。

此外，由于GigaSECURE可在数秒内将设备从带外切换至串接模式，所以我们可以很方便地用实际网络流量来测试安全工具。其中包括:

- 在检测模式下验证升级版安全工具
- 通过生产流量来建立安全基线和网络安全正常行为模型;

一切就绪后，您在瞬间便可将安全工具切回串接模式。

更多有关GigaSECURE Inline Bypass智能引流功能的信息

欲了解GigaSECURE安全交付平台Inline Bypass智能引流功能可为您的网络带来什么优势，敬请访问**www.gigamon.com/gigasecure**.

6116-01 06/18

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