网络入侵防护系统

常见问题

腾讯云

常见问题

最近更新时间：2023-12-28 11:54:11

网络入侵防护系统对比传统安全防御产品有哪些优势?

传统安全防御产品多采取串行的部署方式，针对7层请求进行阻断，可能由于单机性能瓶颈造成整个业务故障。网络入侵防护系统采用旁路部署方式，能够在不影响业务的前提下，无变更、无侵入地对4层的请求进行 ACL 管控，这是传统安全防御产品难以达成的。

网络入侵防护系统对之前已经采购过的其他安全产品、数据分析平台等能否兼容?

网络入侵防护系统各核心组件 API 化，方便客户集成到原有系统中，并通过网络入侵防护系统提升原有系统的安全防御效果。

网络入侵防护系统对 HTTPS 加密协议如何分析和阻断?

网络入侵防护系统可以通过以下两种方式对 HTTPS 加密协议进行分析和阻断。

- 方式一：流量通过 TCE 中的 STGW 转发 SSL 卸载后的流量给网络入侵防护系统平台实现，阻断效果和方式不变。
- 方式二：通过识别 TLS 原数据中源目的 IP、报文的长度和顺序、会话的方向和流量比例等，再结合威胁情报数据库、机器学习算法实现威胁检测。

网络入侵防护系统是否支持自定义防御规则?

目前仅支持 IP 粒度、URL 粒度的自定义防御规则。支持 HTTP 协议中 Cookie、Referer 等7种字段的精细化 ACL 管控。

单机支持多大流量的业务环境?

目前网络入侵防护系统的单机性能可以支持10Gbps 带宽的业务环境。若客户业务带宽需求超过10Gbps，安全治理支持水平扩展。