

网络入侵防护系统 常见问题



腾讯云

【 版权声明 】

©2013–2024 腾讯云版权所有

本文档（含所有文字、数据、图片等内容）完整的著作权归腾讯云计算（北京）有限责任公司单独所有，未经腾讯云事先明确书面许可，任何主体不得以任何形式复制、修改、使用、抄袭、传播本文档全部或部分内容。前述行为构成对腾讯云著作权的侵犯，腾讯云将依法采取措施追究法律责任。

【 商标声明 】



及其它腾讯云服务相关的商标均为腾讯云计算（北京）有限责任公司及其关联公司所有。本文档涉及的第三方主体的商标，依法由权利人所有。未经腾讯云及有关权利人书面许可，任何主体不得以任何方式对前述商标进行使用、复制、修改、传播、抄录等行为，否则将构成对腾讯云及有关权利人商标权的侵犯，腾讯云将依法采取措施追究法律责任。

【 服务声明 】

本文档意在向您介绍腾讯云全部或部分产品、服务的当时的相关概况，部分产品、服务的内容可能不时有所调整。您所购买的腾讯云产品、服务的种类、服务标准等应由您与腾讯云之间的商业合同约定，除非双方另有约定，否则，腾讯云对本文档内容不做任何明示或默示的承诺或保证。

【 联系我们 】

我们致力于为您提供个性化的售前购买咨询服务，及相应的技术售后服务，任何问题请联系 4009100100或 95716。

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护产品有哪些优势？

传统安全防护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，这是传统安全防护产品难以达成的。

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。