

网络入侵防护系统

新手指引



腾讯云

【 版权声明 】

©2013–2026 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。

新手指引

最近更新时间：2026-07-20 17:19:09

本文将为刚入门网络入侵防护系统的用户提供一条学习路径，帮助新手用户快速了解和使用网络入侵防护系统。

1. 网络入侵防护系统概述

网络入侵防护系统（Network Intrusion Prevention System，NIPS）基于腾讯近二十年安全技术的积累，通过旁路部署的方式，提供双向流量逐包检测和 IP 封禁能力，解决数据中心的协同防御和安全治理问题。同时提供阻断 API，方便其他安全检测类产品调用。此外，网络入侵防护系统提供全量网络日志存储和检索、可视化大屏等功能，帮助客户解决等保合规、日志审计、行政监管、以及云平台管控等问题。

2. 了解网络入侵防护系统

您可以依次查阅如下文档，进一步了解网络入侵防护系统：

- [网络入侵防护系统有哪些优势？](#)
- [网络入侵防护系统的应用场景是哪些？](#)
- [网络入侵防护系统核心功能有哪些？](#)
- [网络入侵防护系统产品架构是什么？](#)

3. 网络入侵防护系统计费

网络入侵防护系统的计费模式分为订阅与非订阅，分别适用于不同场景下的用户需求，详情可参见[购买指南](#)。

当您需要购买咨询时，您可以直接通过[售前咨询](#)进行提问，会有专属客户经理在线为您解答，为您提供专业的上云方案。

同时，您也可以直接致电销售人员，咨询热线：4009100100转1（工作日9:00 – 18:00）。

4. 新手常见问题

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。

网络入侵防护系统的阻断原理是什么？

向源 IP 和目的 IP 发送 RST 包干扰网络连接，达到对 TCP 协议的阻断效果。

网络入侵防护系统是否支持自定义防护规则？

支持 IP 防护规则，支持 HTTP 协议中 Cookie、Referer 等7种字段的精细化 ACL 管控规则。

5. 反馈与建议

使用网络入侵防护系统产品和服务中有任何问题或建议，您可以通过以下渠道反馈，将有专人跟进解决您的问题：

- 如果发现产品文档的问题，如链接、内容、API 错误等，您可以单击文档页右侧**文档反馈**或选中存在问题的内容进行反馈。
- 如果您有其他疑问，可前往 [腾讯云开发者社区](#) 进行提问。
- 如果遇到产品相关问题，您可咨询 [在线客服](#) 寻求帮助。