网络入侵防护系统

产品简介

腾讯云

【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。

文档目录

产品简介
产品概述

最近更新时间：2024-09-11 15:39:31

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。

产品功能

网络入侵防护系统的主要功能，如下表所示：

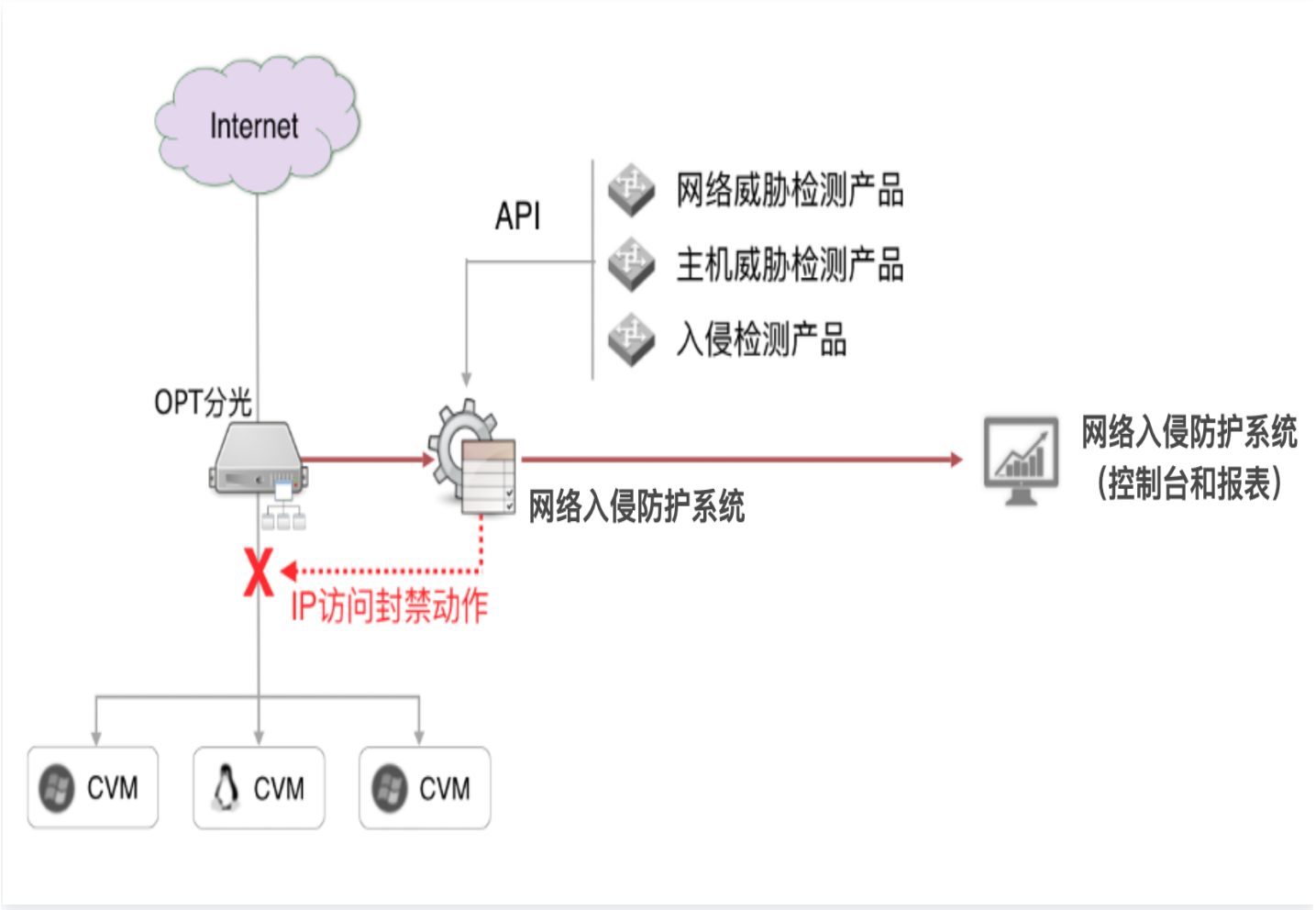
功能	功能描述
黑白名单配置	用户可基于 IP、域名、URL 等维度对网络流量进行管控
联动防御 API	支持 IP、域名、URL 等封禁、解封 API 接口
安全可视化	可视化查看安全总览情况，支持自定义报告内容和导出报告
系统监控	提供平台监控及系统巡检功能

产品架构

最近更新时间：2024-09-11 15:39:31

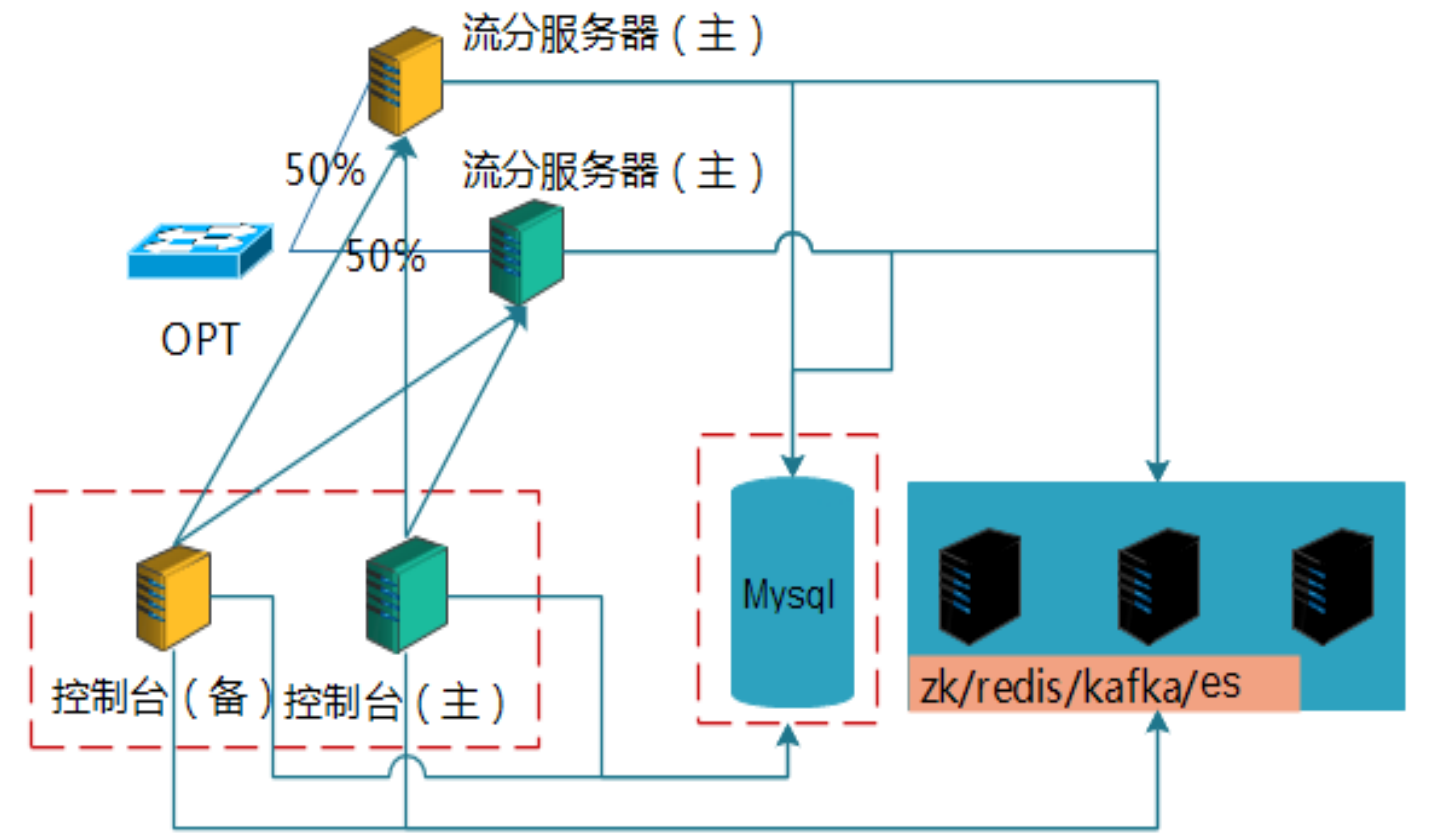
整体示意图

整体结构示意图如下所示：



网络架构图

高可用版网络架构示意图如下所示：



- **流分服务器**：用于流量数据分析、阻断，支持多主部署模式，由 OPT 镜像分配流量。当某台机器故障，网络链路自动与其断开，并将流量切换至另外一条链路，保证流量分析服务不受影响。
- **控制台**：主备模式部署，当主机故障时，自动切换备机对外服务，配合虚拟 IP 使用，可达到自动切换。
- **存储**：包括 MySQL，Redis，ZooKeeper，Kafka，Elasticsearch。
  - MySQL，热备部署模式，当 mysql 主机故障，程序自动切换到备机，保证业务数据传输不中断。
  - redis，zookeeper，kafka，elasticsearch，至少3节点的集群模式部署。任意一台机器故障均不会影响程序正常运行，且支持横向扩容。

产品优势

最近更新时间：2024-09-11 15:39:31

旁路部署

采用旁路部署模式，对业务无侵入，不会引起业务故障。并且提供双向流量逐包检测能力以及IP封禁能力。能够有效解决数据中心的协同防御和安全治理问题。

高阻断率

拥有腾讯专利技术，基于内核协议栈做了深度定制，把旁路阻断技术做到了极致。并且支持同时下发20万条规则，阻断成功率高达99.9%。

网络流量实时监控

支持跨 Region（云区域）的 TB 级双向流量镜像。具备微秒级网络协议解析和毫秒级流量分析的能力。支持 IP、URL 和域名这三个层级的会话实时阻断。

联动开放

核心阻断能力 API 化，并与国内主流厂商完成标准化对接，可将安全设备（生态厂商）接入系统的阻断能力，对已有的安全产品进行整合，提升防御范围。

应用场景

最近更新时间：2024-09-11 15:39:31

合规护网保障

问题场景

针对内外部红蓝对抗、网络安全评测等行动，如“等保测评”、“护网行动”，需要日志审计和全局攻击源封禁功能。

解决方案

采用旁路部署的方式，不影响业务的同时，提供双向流量逐包检测，通过向源 IP 和目的 IP 发送 RST 包干扰网络链接，达到对攻击 IP 的阻断效果。

安全能力协同

问题场景

现有的安全产品不能完成阻断，提供 IP 封禁 API，给其他检测类产品调用。

解决方案

提供第三方安全设备联动防御 API，将系统的阻断能力开放给其他检测类设备等产品调用并下发阻断，盘活企事业单位现有的安全设备能力，实现协同防御，形成响应防御中心，与其他厂商的安全产品组合使用，适用更多使用场景。

威胁情报联动防护

问题场景

依托海量的高质量威胁情报服务，对网络恶意流量进行精准判定，提升防护能力。

解决方案

与海量威胁情报优势相结合，由腾讯统一的威胁情报中心向客户共享，客户能够第一时间更新策略，完成预防和应急，从而实现“一点感知、全网联动”。并内置数百种网络分析模型，能准确识别异常主机、恶意攻击等。

虚拟补丁防护

问题场景

在日常运维期间，不时会有一些 0Day、1Day 以及 CVE 漏洞，且官方还未来得发布修复或短时间较难进行修复。

解决方案

提供部分七层防护能力，针对重大保障活动期间的威胁及漏洞，帮助客户能及时修补防护漏洞，配置策略。通过先拦截阻断再推进修复的方式临时缓解漏洞影响，及时合理的安全运营帮助守护网站层出不穷的 Web 漏洞隐患，保障业务系统安全，给漏洞修复留下时间。

秒拨IP攻击防护

问题场景

IPv6时代攻击成本日趋下降，防守方急需补充对海量请求地址的防护能力。

解决方案

通过 AI+算法聚合分析攻击指纹，构建精准防护模型，识别并封禁如薅羊毛等秒拨 IP 攻击。通过防护模块提取正常用户和秒拨攻击者流量指纹，若匹配到黑指纹库，则发送双向 RST 包进行旁路阻断。