KEMYOND

CDKY-IDS9000

工业入侵检测系统

特点和优势

- 全面支持 IPV6
- 多业务高性能
- 成熟的流检测技术，提升性能和准确性
- 文件上传过滤
- 便捷的管理方式

介绍

宽域网络入侵检测系统（IDS）具有安全审计、监视、攻击识别、防蠕虫和防攻击等多项功能，能对外部攻击、内部攻击和误操作进行实时监控，是网络系统纵深防护的必要手段，在网络安全防御体系中具有不可替代的作用。

宽域网络入侵检测系统采用专用硬件平台，负责网络数据的获取、分析、检测，对违反安全策略的行为进行识别、合并、记录，实时发送报警信息到监控中心，通过 WEB 浏览器、监控中心获取实时报警信息，亦可查阅、分析历史报警信息，还可定制检测策略、响应策略和控制检测引擎。

规格

接口配置

接口配置	RJ45*10，10/100/1000Base-T(X)self-adaption 2 个千兆 combo 口
USB	USB 1.0 secret key (two-factor authentication)
管理口	1*1000M/100M RJ45 in-band management

性能特性

还原能力	支持对 HTTP、FTP、POP3、Telnet 等主要的网络协议通信内容进行恢复和还原； 支持采用双协议栈架构，支持 IPv6/IPv4 双协议栈功能，能同时识别 IPv4 和 IPv6 通讯流量，并对 IPv4 和 IPv6 流量进行安全检测。 当背景数据流低于网络有效带宽的 80%时，系统能够保证数据的获取和还原能够正常进行。

产品功能

网络适应性	支持在线检测模式、旁路监听检测模式，并支持多路监听并发检测。
入侵检测	支持基于 IP 碎片重组、TCP 流重组、会话状态跟踪、应用层协议解码等数据流处理方式的攻击识别；支持模式匹配、异常检测、统计分析，以及抗 IDS/IDS 逃逸等多种检测技术；支持 IDS 报文取证。
特征规则	内置攻击特征库，特征数量超过 8,500 余条，定期更新特征库；可基于 TCP/ICMP/UDP 协议自定义攻击特征，可阻挡蠕虫、木马、间谍软件、广告软件、缓冲区溢出、扫描、非法连接、SQL 注入、XSS 跨站脚本、Webcgi 攻击检测、信息泄露攻击检测等多种攻击。
协议状态分析	支持 Telnet、FTP、HTTP、SMTP、SNMP、DNS 等多达 30 种的主流应用层协议。
事件统计分析	攻击事件显示：实时显示攻击事件，及按照时段分类统计和严重程度统计等信息。报表分析：提供多种报表，可依据五元组、应用协议、时间点/时间段等元素自定义报表内容并显示。 告警通知：可对接口流量/应用/协议的异常状态进行告警，并以 Email/SNMPtrap/声音等方式通知管理员。
文件上传过滤	内置病毒过滤引擎和实时更新的病毒特征库，可以对通过 HTTP 和 FTP 协议上传的文件进行病毒检测，发现恶意文件进行实时告警，防止恶意文件造成更大的影响。
管理方式	支持本地管理和远程管理，支持本地串口及 HTTPS、SSH 等加密方式管理，在各种环境下均可方便的进行运维管理工作。

机械特性

机箱外壳	高强度机箱表面散热，无风扇设计
防护等级	IP40
尺寸（W×D×H）	440mm x 263mm x 44mm
安装方式	1U 机架

质量保障

保修期限	2 年
MTBF	>350000h

订购信息

型号	千兆网口	千兆combo口	Console	USB	尺寸	网络层吞吐量	IDS吞吐量	电源
CDKY-IDS9000	10	2	1	1	1U	3Gbps	800Mbps	单电源

上海宽域工业网络设备有限公司

上海市宝山区园丰路69号3幢5层

189-1779-7159 (技术支持)　021-56561181 (座机)

189-1819-0263 (销售咨询)　zhouaixia@kemyond.com (邮箱)

成都研发中心

成都市高新区天府大道北段1480号孵化园6号楼105号

028-86263902 (座机)

官方网站

www.kemyond.com

宽域公众号