力控科技 FORCECON | HUACON 力控华康

华康网络
入侵检测系统
HC-IDS

北京力控华康科技有限公司

www.sunwayland.com

目 录

产品概述

近几年来，随着互联网+、业务数字化转型的深入推进，面对层出不穷的新型安全事件如网站被篡改、被挂黑链、0 day漏洞利用、数据窃取、僵尸网络、勒索病毒等等，传统安全建设模式已经捉襟见肘，面临着巨大的挑战。

如何能够及时发现网络入侵的发生，并合理、规范化的利用现有的网络资源，成为摆在我们面前的一个重大问题。

华康网络入侵检测系统**集实时入侵检测、病毒检测、僵尸网络检测、敏感信息检测、DoS/DDoS攻击检测、p2p流量检测等多项高级功能于一体**。它采用先进的技术体系和高效的入侵检测技术，包括以全面深入的应用层协议分析技术为基础，TCP流重组、IP碎片重组、会话重组、协议识别与还原、特征检测、协议异常检测、攻击关联分析为核心的高性能入侵检测引擎，通过综合采用标记检测、协议分析、后门检测、流量签名、欺骗检查、链路层检查、连接风暴检测、内容分析和异常行为分析等相结合的多种检测技术，提高检测的准确度和有效性，实时发现网络中的恶意流量和垃圾流量，保护信息资产安全。

> “集实时入侵检测、病毒检测、僵尸网络检测、敏感信息检测、DoS/DDoS攻击检测、p2p流量检测等多项高级功能于一体。”

产品架构

华康网络入侵检测系统基于自主研发的安全操作系统，其采用多核并行处理架构。架构内部将数据平面与控制平面进行分离，形成多个控制平面和数据平面，每个数据平面占用一个CPU核心实现数据快速处理检测，各数据平面之间的协议栈互不影响。每个独立的控制平面包含多个安全引擎实现安全检测，包括应用识别、漏洞攻击检测、僵尸网络检测、病毒检测、WEB应用检测、URL分类检测、数据防泄漏、DDOS检测等。

系统包含五个主要组件：网络数据引擎、网络安全引擎、安全防护模块、审计中心、管理模块，为各种网络环境提供灵活的部署和管理。

产品特点

检测全面，IPv6支持

华康网络入侵检测系统旁路部署在网络中，支持IPv4及IPv6网络环境。它通过综合采用标记检测、协议分析、后门检测、流量签名、欺骗检查、链路层检查、连接风暴检测、内容分析和异常行为分析等相结合的多种检测技术，提供准确的检测和阻断，以发现已知和未知攻击。

智能化识别应用

华康网络入侵检测系统内置应用识别库，支持9700+种应用识别。在配置界面上为用户提供应用列表，并按照使用维度对应用进行分类，包括web流媒体、P2P下载、网络游戏、即时通讯、网络存储、网上支付、数据库等37个类别，并且支持达梦、南大通用、神通等国产数据库协议的识别和控制。

对于特征不明显、较难识别的应用或者未知类型的应用，比如P2P类型的应用，系统提供了应用智能识别功能，该功能是应用特征识别的补充，可按照数据连接的频率、地址及端口变化、数据包负载大小等因素综合考虑进行应用的动态识别和控制。

一体化安全检测策略

华康网络入侵检测系统在一条安全策略中即可全部或部分选择：应用行为识别、漏洞攻击检测、病毒检测、僵尸网络检测、Web应用检测、敏感信息检测。免去用户以往在多个不同安全配置页面间频繁切换，重复配置的不便。在其它入侵检测产品上需要配置多达6条策略才能实现的功能，在华康网络入侵检测系统上只需要一条安全策略即可完成，且逻辑上更加清晰简单，便于理解，极大的提高了管理易用性和可维护性，防止了繁琐配置引起的错误风险。

应用层深度防护

• 漏洞攻击防御

华康网络入侵检测系统内置7000+威胁特征库，按照攻击手段将威胁入侵分为21大类，分别为可network_device漏洞攻击、media漏洞攻击、dns漏洞攻击、tftp漏洞攻击、ftp漏洞攻击、web漏洞攻击、mail漏洞攻击、database漏洞攻击、scan漏洞攻击、shellcode漏洞攻击、telnet漏洞攻击、file漏洞攻击、web_browse漏洞攻击、web_activex 漏洞攻击、application漏洞攻击、system漏洞攻击、口令暴力破解、worm漏洞攻击、trojan漏洞攻击、spyware漏洞攻击、backdoor漏洞攻。

华康网络入侵检测系统可防护远程扫描、暴力破解、缓存区溢出、蠕虫病毒、木马后门、SQL注入、跨站脚本、web攻击等各种网络及应用攻击。对于“永恒之蓝”、“震网三代”、“暗云3”、Struts”、Struts2”、Xshell 后门代码”、“勒索”等新型漏洞攻击可实时进行识别和阻断。并能够对检测到的入侵事件采取实时告警、阻断、手动确认、等多种防护措施，同时记录事件详细信息和提供统计报表。漏洞规则还支持用户自定义规则，建立规则组等功能。

• URL过滤

华康网络入侵检测系统具备丰富的内置URL分类库，包含按照不同类型（如不良言论、色情暴力、网络钓鱼、论坛聊天等）划分的超过上亿条记录的URL信息，可实现对工作无关网站、不良信息、高风险网站的准确、高效过滤。

同时华康网络入侵检测系统内置的Web信誉库，通过对互联网站点资源（域名、IP地址、URL等）进行威胁分析和信誉评级，将含有恶意代码的网站列入Web信誉库，可有效检测用户对挂马等不良信誉网站的有意或无意访问，实现对终端用户的安全检测。

• 病毒检测

华康网络入侵检测系统采用流模式和启发式文件扫描技术，对利用HTTP、SMTP、POP3、FTP、IMAP、SAMBA、IM等多种协议进行传播的病毒进行扫描，完成对木马病毒、蠕虫病毒、宏病毒、脚本病毒、僵尸网络程序等的查杀，同时支持多线程并发控制、深层次压缩文件杀毒等功能。

此外，华康网络入侵检测系统将专业防病毒引擎和多核并行处理技术完美融合，实现高速病毒处理性能。

• Dos/DDos防护

华康网络入侵检测系统能够有效地检测常见的Dos/DDos攻击手段，包括SYN Flood、UDP Flood、ICMP Flood、RST Flood、ACK Flood、DNS Flood、HTTP Flood等洪水攻击，以及Teardrop、WinNuke、Land、Smurf、Fraggle等畸形报文攻击。

• 敏感信息检测

系统通过内容安全关键字，可对任意安全区域间交互的网页内容、搜索引擎信息内容、文件传输（文件名、格式、内容）、邮件收发（包括收发人、标题、内容、文件等）、论坛发言、服务器操作以及即时通讯内容等进行基于内容关键字的准确检测、告警、记录和信息还原，实现深度内容安全管理与跟踪。

关联分析

华康网络入侵检测系统支持对威胁日志的深入分析，支持行为关联以及异常事件的关联挖掘分析，支持内网资产被攻击过程展示(目标定位、目标扫描、提升权限、病毒投递、安装后门)，源威胁度分析，可以判断未知攻击。

资产风险识别

华康网络入侵检测系统可根据用户指定的网段或主机范围，通过主动扫描分析技术，识别出如操作系统版本漏洞威胁度、上网浏览器客户端漏洞威胁等信息，让用户实时了解当前网络资产中的脆弱性，勾勒脆弱性全景图，并可针对性的实施漏洞填补，升级补丁，访问控制，流量监控等安全措施，从而达到防范潜在入侵攻击的可能性。通过系统提供的资产脆弱性视图，结合当前流量分析后的安全事件告警进行关联，可详细展示当前网络被入侵主机数量、时间、威胁类别、情报来源、IP、用户名、资源、威胁简介、资产详情等统计信息。

智能联动功能

华康网络入侵检测系统支持和华康安全云进行对接，对于本地识别不了的可疑文件及应用特征，上传云端以实现云查杀、云联动、URL云识别、应用云识别、威胁情报云检测，并实时将云端最新防护规则更新到本地，实现协同防御。支持和华康态势感知、沙箱、APT、SOC、漏洞扫描系统、网站监测等产品进行信息共享和策略联动，构建内外网整体安全防御体系。

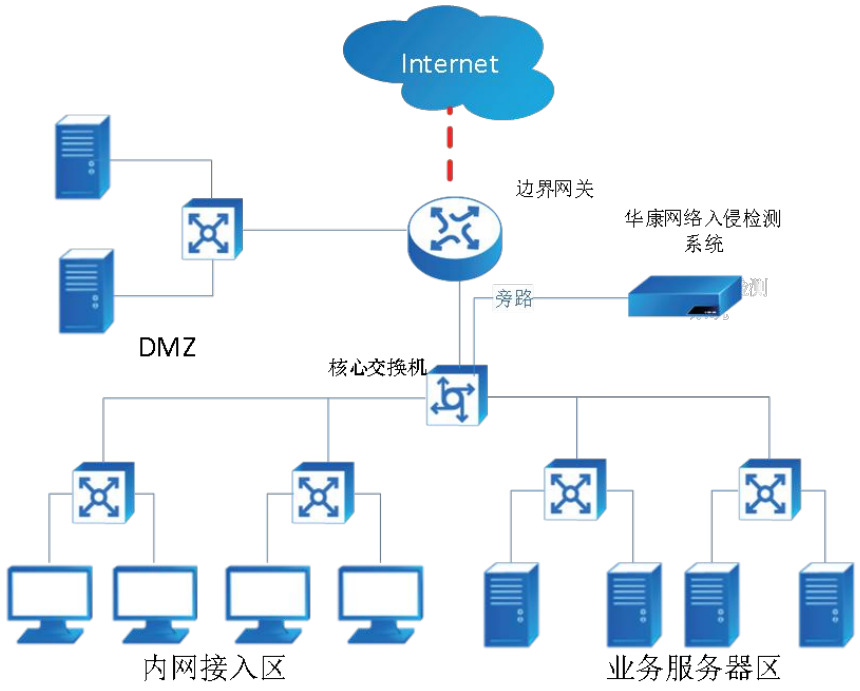
全面可视化数据展示

华康网络入侵检测系统的数据中心记录、展示和统计各种日志以及威胁事件信息。用户可以及时查看设备的运行状态、管理操作记录以及网络中存在的各种威胁事件。系统提供可视化的威胁事件、攻击事件、用户流量情况、应用事件、漏洞风险、用户资产等的展示和安全审计功能，并提供了威胁、业务、用户、风险、四个角度的分析报告，方便用户掌握当前所防护网络的安全状况。分析报告可定期自动生成，也可手动立即生成。

典型应用

华康网络入侵检测系统的应用方式简单，能够快速部署在几乎所有的网络环境中，实现从企业网络核心至边缘及分支机构的全面保护，适用于不同环境不同企业的安全需求。

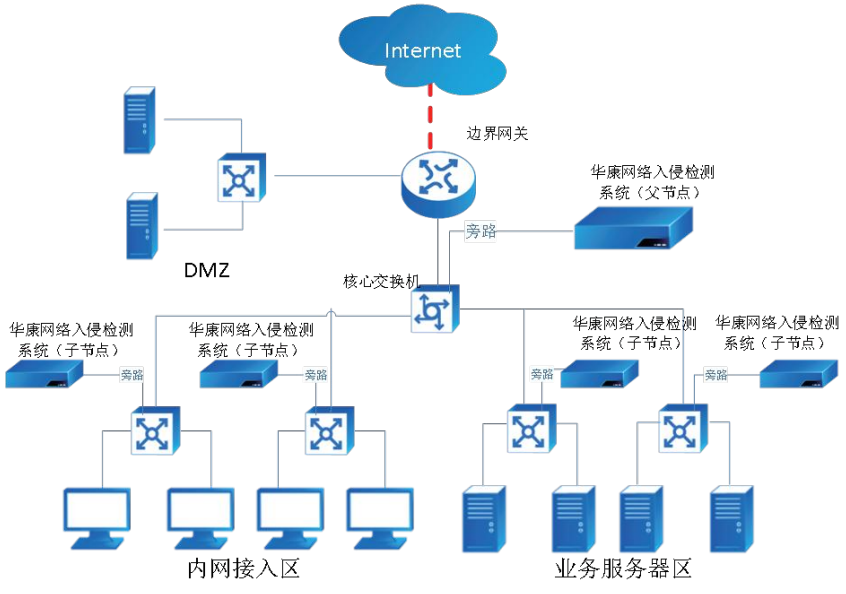
旁路部署典型应用



分布式部署典型应用

针对大型网络环境，华康网络入侵检测系统支持分布式部署、集中式管理。针对来自外部和内部的攻击，华康网络入侵检测系统提供在线防护的部署方式，通过将系统部署在关键网络链路上，实时检测数据流量中各种类型的恶意攻击流量，保护企业的重要信息资产。

华康网络入侵检测系统分别部署在各个网络区域，华康网络入侵检测系统（子节点）都会将日志信息统一发送到华康网络入侵检测系统（父节点）上，华康网络入侵检测系统（父节点）对这些日志进行统一的分析和处理，从而使得网管人员能够掌握企业网络的整体安全状况和全局流量分布。



力控科技 FORCECON

北京力控华康科技有限公司

地址：北京市海淀区天秀路10号中国农大国际创业园1号楼
总机：010-62839678
全国统一服务热线：400 650 1353
www.huacon.com.cn

关注公众号　关注小程序