AVCOMM™恩创®

入侵检测系统
Datasheet

恩创致力于将先进的信息技术带入工业控制与工业信息领域。

安通恩创信息技术（北京）有限公司 www.avcomm.cn

电子邮箱: sales@n-tron.com.cn

电话： （010）- 82859971

地址：北京市海淀区马甸东路19号金澳国际公寓3105

产品概述

恩创入侵检测系统是集入侵检测、入侵防御产品于一体，依照安全策略对工业网络系统的运行状况进行监视，发现并阻断各种入侵攻击、异常流量、非法操作或异常行为的软硬件一体化设备。产品通过深入分析网络上捕获的数据包，结合特征库进行相应的行为匹配，实现入侵行为检测和防御、病毒恶意代码查杀、web攻击防护、安全风险评估、安全威胁可视化等功能。部署入侵检测系统可以及时发现来自生产网外部或内部违反安全策略的行为及被攻击的迹象，通过告警提醒工业用户及时采取应对措施，最终达到保障生产网络安全运行的目的。

产品亮点

兼容主流工控系统

产品具备与多家主流工控厂商的兼容性测试报告，具有丰富的硬件接口，双电源设计，完全满足工控现场复杂的应用需要，能与行业主流工控系统厂商DCS、SCADA等控制系统完美兼容。

强大的入侵检测系统

内置通过超过4000种预定义的攻击特征库，结合多核硬件架构和流检测技术对各类应用进行深入分析，具备针对已知通用应用协议或应用系统漏洞的攻击行为检测和防护，同时产品还支持病毒和恶意代码查杀、WEB攻击防御等应用层安全防护能力。

全面支持IPV6

FTP多通道、应用审计与管控、URL过滤与恶意URL过滤、IPS、防病毒等应用全面支持IPV6，支持IPV6数据包安全检测机制，可有效预防异常包攻击；支持IPv6环境，可创建IPv6地址和地址范围，支持展示地址对象被引用次数，支持NAT64。

灵活的安全策略管理

产品采用基于策略的防护方式，内置了多种默认安全策略集，用户可以根据需要选择最适合自己需要的策略，以达到最佳防护效果。用户即可以根据防护的类型不同而选择不同的事件集，即可以提高系统的性能，也可以减少误报的发生机率。

检测防御一体化设计

支持透明、旁路、桥模式、混合、双机冗余等多种部署方式，可以根据实际情况进行灵活的组合和搭配。既可以旁路部署实现攻击行为的攻击报警，也可以直路串接实现攻击行为的实时阻断，一台设备同时支持入侵检测和入侵防御混合部署。通过集中管理平台可将分布于不同地理位置的多个设备进行聚合性的统一安全防护。

产品功能

部署模式

- 支持旁路模式、路由模式、透明（网桥）模式、混合模式，支持多个物理网口加入一个网桥中；
- 部署模式切换无需重启设备；
- 旁路模式下支持多个镜像口流量汇聚分析；

风险扫描

- 支持针对IP、端口进行端口扫描并呈现扫描结果，可选择立即执行或定期执行；
- 支持呈现扫描结果，包括端口、端口状态、端口服务、程序版本、操作系统、风险状态、设备类型和时间等信息，且可以进行导出；
- 支持弱口令扫描，可针对IP、IP端、端口等对象，扫描监控空密码、用户名密码相同、预置弱口令、自定义弱口令等规则；

安全事件监控统计

- 支持攻击趋势图选择性展示及浮动详情查看；
- 支持攻击源地址TOP 10 GIS地图和攻击目的地址TOP 10 热力图展示及浮动详情查看；
- 支持20余种安全威胁数量的分布饼状图展示及浮动详情查看；
- 支持接口相关信息实时展示；
- 支持用户流量TOP10相关信息的柱状图展示；

SSL加密内容审计

- 支持HTTPS解密功能，支持管理界面及命令行配置解密策略；
- 支持HTTPS域名库，预定义域名以及自定义域名；
- 支持针对HTTPS网站、HTTPS门户搜索等内容进行还原；

基于资产的风险识别

- 支持开启或关闭内网资产功能，开启后自动评估内网资产安全，无需人工干预；
- 支持展示风险等级、IP、操作系统、浏览器、应用、杀毒软件、服务等内容；

非法外联防护

- 支持非法外联学习和防护特性，可定义外联白名单地址和端口；
- 支持通过流量自学习能获得服务器合法的外联行为，检测流量中的异常访问流量，可以自动拦截；

DNS透明代理

- 支持DNS透明代理；
- 支持DNS负载均衡；
- 支持DNS静态域名映射；
- 支持DNS特定域名请求转发；

产品功能

威胁检测及防御

- 内置8000多条入侵攻击规则库，支持自定义规则
- 支持拒绝服务、木马后门、间谍软件、蠕虫病毒、缓冲区溢出、安全扫描等网络层攻击检测及防护
- 支持HTTPS防护、DDoS攻击、Web攻击、0-day攻击、CGI攻击等应用层攻击检测及防护；
- 支持1500万余种病毒查杀，病毒库定期更新
- 支持SQL注入、系统命令注入、LDAP注入、SSI注入、邮件注入、请求体PHP注入WEB攻击行为检测防御；

IPV6

- 支持IPv6环境，可创建IPv6地址和地址范围，支持展示地址对象被引用次数；
- 支持针对IPv6报文进行管理和防护，包括应用、URL、入侵攻击、病毒行为等内容；
- 支持IPv6数据包安全检测机制，可有效防御异常包攻击；
- 支持NAT64

SNMP

- 支持v1、v2、v3版本;
- 支持对SNMP用户进行增删查改；
- 通过None、MD5、SHA认证方式对SNMP用户进行认证

用户认证策略

- 支持本地WEB认证、Portal认证、ePortal+SAM认证、短信认证、微信认证、免认证、混合认证；
- 支持混合认证：微信认证、短信认证、本地认证、免认证四种方式混合；
- 支持基于源接口、源地址、目的接口、目的地址、时间多个维度的条件匹配；

系统维护

- 支持三权管理方式，包括权限管理员、账号管理员、审核官和管理员，各管理员权限制约；
- 支持设备管理端口的自定义，包括HTTPS、HTTP、TELNET、SSH等常用管理方式的端口；

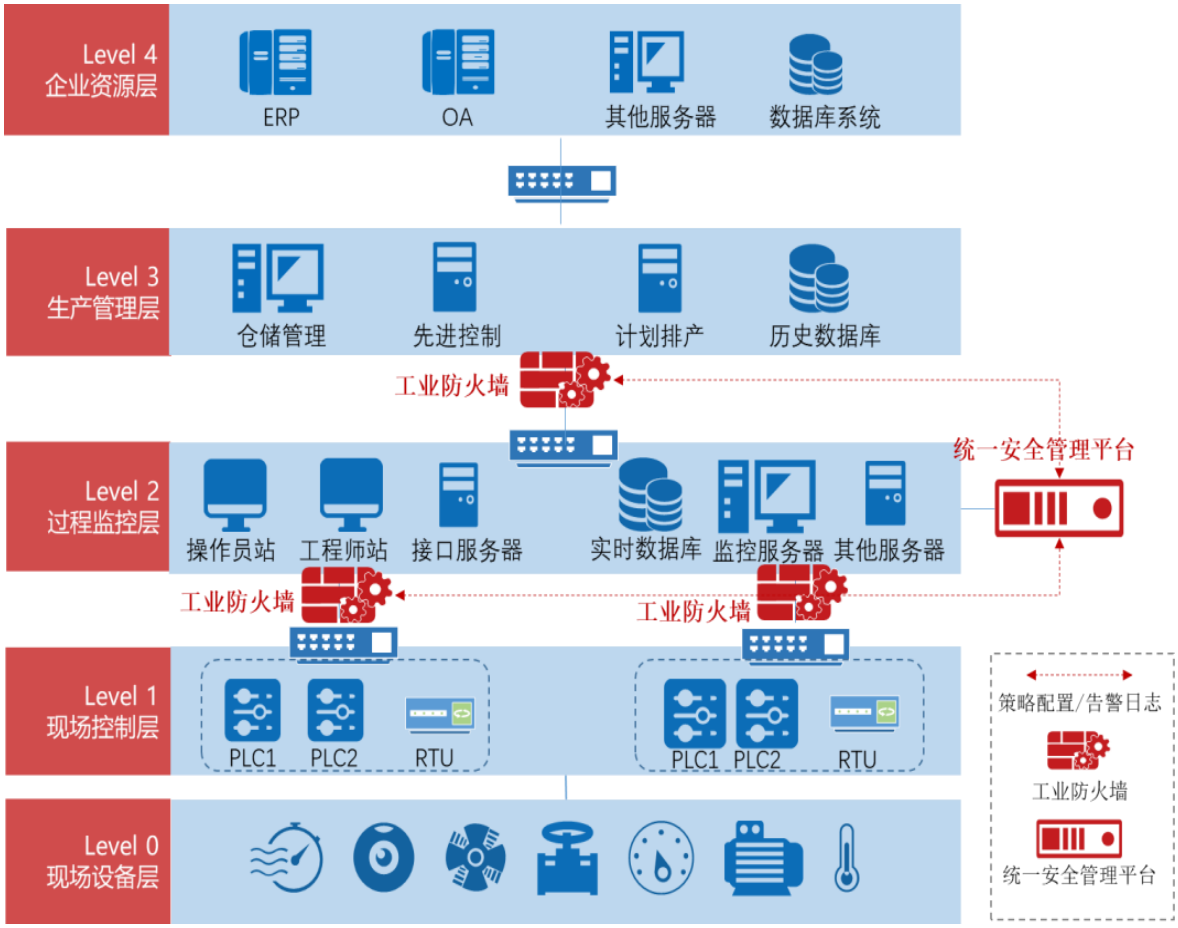
配置管理

- 支持U盘零配置上线，设备端无需预配置，将U盘插入设备USB接口中，即可实现快速上线实施；配置文件内容支持加密；
- 支持按需升级系统版本，可自动快速升级系统版本；
- 支持导入多份配置文件，用于业务需求，变更业务运行，保障可靠性；

产品规格

型号	IDS1012	IDS1024	IDS1026
管理接口	任一业务接口	带外管理GE口	带外管理GE口
固定业务接口	2GE(Combo)+10GE(电)	12GE(电)+12GE（光）	12GE(电)+12GE（光）+2万兆
Console口	1*(RS232 RJ45)	1*(RS232 RJ45)	1*(RS232 RJ45)
扩展插槽数量	无	无	无
BYPASS（对）	支持1对Bypass（GE0和GE1）	支持1对Bypass（GE0和GE1）	支持1对Bypass（GE0和GE1）
硬盘	500G	500G	1T
电源1+1备份	无	有	有
平均无故障时间（MTBF）	≥100,000小时	≥100,000小时	≥100,000小时
缺省配置重量	2.9kg	3.2kg	5.2kg
外形尺寸（长*高*深/mm）	440*44*263	440*44*263	440*44*300
温度	存储温度-40℃~70℃，工作温度0℃~40℃	存储温度-40℃~70℃，工作温度0℃~40℃	存储温度-40℃~70℃，工作温度0℃~40℃
湿度	工作5%-90%非凝露	工作5%-90%非凝露	工作5%-90%非凝露
输入额定电压	100~240V AC	100~240V AC	100~240V AC
最大输入电流	0.6A	2A*2	2A*2
最大功率（W）	25W	120W	120W

应用场景



生产执行层入侵行为检测

- 以旁路方式部署在生产执行层与企业管理层之间
- 实时检测来自办公网及互联网网络流量中的恶意入侵、漏洞利用、非法外联等异常行为，并进行告警
- 详实记录一切进入生产执行层的恶意攻击的网络流量，为安全事故调查取证提供依据

过程监控层行为检测

- 以旁路方式部署在过程监控层与生产执行层之间
- 实时检测来自过程监控层内部违反安全策略的异常可疑行为，并进行告警
- 用流检测、应用内容特征、应用行为特征及关联分析等多种手段对各类应用进行深入分析
- 采用多种协议异常检测技术，并采用全并行处理方式，保证超低的误报率和漏报率