

CDKY-FW3000-G4-GT4

机架式工业防火墙



特点和优势

- 对违规操作及时报警或阻断
- 工控协议深度解析
- EMC 电力 IV 级，无风扇散热设计
- 宽温工作能力（-40℃- +85℃）
- 满足《GBT 37933-2019 信息安全技术 工业控制系统专用防火墙技术要求》

介绍

宽域工业防火墙应《信息安全等级保护管理办法》（公通字【2007】43号）和《信息安全技术网络安全等级保护技术标准》2.0版本而出，旨在为工业互联网提供良好的防攻击能力，一定程度上防止或者减轻 DDoS 攻击，并提供安全审计和日志记录，为工控网络的边界安全保驾护航。

规格

接口配置

接口配置	RJ45*4, 10/100/1000Base-T(X)self-adaption SFP*4,1000Mbits
USB	USB 2.0 secret key (two-factor authentication)
Bypass	2 组
管理口	1*1000M/100M RJ45 in-band management

性能特性

吞吐量	<p>在只有一条允许规则和不丢包的情况下：</p> <p>对 64 字节短包，百兆工业防火墙应不小于线速的 30%，千兆工业防火墙应不小于线速的 40%；</p> <p>对 256 字节中长包，百兆工业防火墙应不小于线速的 70%，千兆工业防火墙应不小于线速的 80%；</p> <p>对 512 字节中长包，百兆工业防火墙应不小于线速的 90%，千兆工业防火墙应不小于线速的 95%；</p>
延迟	在吞吐量 90%条件下：

	<p>对 64 字节短包、256 字节中长包、512 字节长包，百兆工业防火墙平均延迟不应超过 1ms。</p> <p>对 64 字节短包、256 字节中长包、512 字节长包，千兆工业防火墙平均延迟不应超过 200us。</p>
最大并发连接数	<p>百兆工业防火墙的最大并发连接数应不小于 60000 个；</p> <p>千兆工业防火墙的最大并发连接数应不小于 300000 个；</p>
最大连接速率	<p>百兆工业防火墙的最大连接速率应不小于 1500 个/s；</p> <p>千兆工业防火墙的最大连接速率应不小于 5000 个/s；</p>

主要功能

基础特性	<p>支持基于源 IP、目的 IP、源端口、目的端口、协议类型、源 MAC、目的 MAC 七元组及时间段的访问控制功能，支持状态检测，支持基于 IP 组的连接数限制，策略支持地址对象。</p> <p>支持双向 NAT，可实现 SNAT 的“多对一”地址转换，实现内网地址的隐藏；DNAT 应至少可实现“一对多”地址转换，能够应用于工控系统内部 DMZ 区服务器对外提供服务的业务场景。</p> <p>支持安全域功能，预置 trust、dmz、untrust，并可自定义安全域。</p> <p>支持静态路由与策略路由，支持桥接口、子接口、VLAN 等网络功能。</p> <p>支持网络时钟同步功能，可扩展支持 B 码时钟同步。</p>
支持工控协议白名单	<p>支持智能学习和自定义结合的方式构建工控协议白名单规则，进行指令级乃至值域级的控制，从而达到阻断异常指令和可疑操作的目的。</p>
工控协议深度解析	<p>支持 5 种以上常见工业协议如 OPC、Modbus(TCP/UDP)、IEC104、DNP3、Profinet、MMS、S7、GOOSE、SV、CIP 等工控协议识别，报文最深达值域级的深度解析，支持报文格式检查，动态端口识别。</p> <p>支持自定义应用类型的二次开发，可以对私有协议或者常用工控协议私有字段的自定义进行识别。提供对第三方工控协议的深度解析和二次开发样例，方便实现协议深度解析与扩展。</p> <p>工控威胁检测库：实时检测工控网络中的攻击行为，通过内置的工控威胁库及威胁特征检测规则，实时对网络中的入侵进行识别、处置并告警和生成相应日志。</p>
流量分析可视化	<p>对所有通过防火墙上的实时数据流量进行实时显示，并按照设备、MAC、IP 地址、网络服务、时间和协议类型等维度进行分析统计，包括流量占比图表、实时流量趋势图、平均流量等，能够对流量超过预警值的行为进行告警和生成相应日志。</p>
实时网络拓扑图	<p>展现已接入网络产品设备，并对设备进行统一布局，动态增加新接入设备，查看布局时一目了然，也可根据现场需求设计定制化布局，实时监测网络。支持多种查询接口。</p>
安全审计	<p>支持日志级别的设定，至少须包括调试、信息、警告、错误四个级别。</p> <p>针对目前各行业广泛的态势感知平台、日志分析平台支持提供日志信息给第三方日志平台。</p> <p>支持生成国网规范格式的日志。</p>

系统自身安全性	<p>管理员须支持两种或两种以上的身份鉴别模式，支持通过安全管理平台的集中管控和管理用户权限的三权分立。</p> <p>基于 SSL 的远程管理：通过网络可以直接对工业防火墙进行管理和配置。通讯采用了 SSL 加密技术，所有配置管理信息在网络上全部以密文传输，可以防止恶意攻击者使用网络监听工具窃取信息。</p>
系统高可用性	<p>设备采用工业级硬件设计，具有较强的环境适应性。</p> <p>支持硬件 Bypass 功能，触发该功能时可及时告警。</p> <p>启动时进行自检，发现异常及时告警，并对程序文件或配置文件的异常提供一定的恢复功能。</p>

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 315mm x 44mm
安装方式	1U 机架

电源参数

输入电压	90-265VAC,130V~375VDC
电源冗余	双电源
功率	<18w
保护	反接保护、过载保护

工作环境

工作温度	-40°C - +70°C
保存温度	-40°C - +70°C
相对湿度	5%-95%无凝结

指示灯

电源指示灯	P1、P2
运行指示灯	RUN
告警指示灯	HDD

行业标准

EMC	<p>电 IEC61000-4-4(EFT)</p> <p>IEC61000-4-5(Surge)</p> <p>IEC61000-4-2(ESD) ±8kV(contact), ±15kV(air)</p>
-----	--



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