Ruijie Networks 锐捷

RG-IDP-P系列

入侵检测防御系统

01 产品概述

随着社交网络、云计算、大数据等新兴技术的蓬勃发展，互联网正经历着前所未有的繁荣时期。然而，这种繁荣也带来了更为复杂多变的信息化安全问题，使得传统的安全建设模式遭受了前所未有的挑战。为了应对这一严峻形势，锐捷网络凭借对市场需求的深刻理解以及多年积累的技术优势，结合“入侵检测防御系统”的最新发展趋势，成功推出了其新一代RG-IDP-P入侵检测防御系统。

RG-IDP-P系列入侵检测防御系统是锐捷网络针对当前网络环境下安全威胁的多样化、隐蔽性和高发性而精心打造的安全解决方案产品。该系统不仅具备传统入侵检测与防御功能，更融入了先进的威胁情报、大数据分析、机器学习等先进技术，从而实现了对安全威胁的精准识别、快速响应和有效防御。

在具体功能上，RG-IDP-P系列系统能够实时监测网络流量，及时发现并阻断恶意攻击和入侵行为。提供主动资产发现、智能策略管家、一键故障分析功能来简化产品上线及运维；具有丰富的安全功能，能够支持入侵防御、防病毒、端口扫描、流量学习、应用控制、DoS/DDoS防护、威胁情报的等功能；支持云平台统一管理、数据同步云端分析与报告、远程监控与运维。同时，该系统还能够对潜在的安全风险进行预警，为网络安全管理员提供及时、准确的安全威胁信息。此外，通过与锐捷网络其他安全产品的协同工作，RG-IDP-P系列系统还能够构建出更加完善、立体的安全防护体系，提升网络的整体安全水平。

在性能表现上，RG-IDP-P系列系统采用了高性能的硬件平台和优化的软件算法，确保了在高流量、高并发环境下的稳定运行和高效检测。同时，RG-IDP-P系列入侵检测防御系统具备性能扩展能力，通过购买性能授权进行扩展，提供丰富的配置选项和灵活的部署方式，以满足不同规模和类型网络的安全需求。

02 产品外观

RG-IDP-P8600-G20
右前俯视图

RG-IDP-P8600-G20
右后俯视图

03 产品特性

统一的安全防护

RG-IDP-P系列入侵检测防御系统集合统一的安全防护功能，包括防火墙、防病毒、入侵检测防御、威胁情报、应用识别、URL过滤等模块，以满足等级保护要求；支持SYN、UDP、ICMP等洪水型DoS/DDoS攻击防护，支持ARP攻击防御功能；支持对HTTP、TCP、UDP、DNS、TLS等常用协议及应用的攻击检测和防御，支持对欺骗攻击、注入攻击、中间人攻击、跨站请求伪造、跨站脚本攻击、代码执行、释放重利用等多种类别的威胁进行检测和防御。病毒防护功能集成

海量病毒库及双引擎查杀，可满足用户快速查杀与深度查杀需求。威胁情报立足于本地大容量出站情报，可及时、高效、准确拦截异常流量。

硬件安全方面，硬件高性能抗拒绝服务攻击，抗攻击一个顶俩。入侵检测防御系统CPU内嵌特有的抗拒绝服务攻击硬件，不同于市场同档次产品的常见软件抗攻击，把抗攻击交由专有硬件处理，抗拒绝服务攻击的性能至少翻一番，让网络更健壮、更安全。

大容量本地威胁情报库

随着出站安全防御的发展，从第一代IPS/入侵防御，基于特征指纹库识别安全风险，对新型变种攻击（勒索、挖矿、钓鱼等）拦截效果差，到第二代的防火墙/入侵检测防御系统+云端威胁情报方式，基于防火墙/入侵检测防御系统与超大容量的云端威胁情报库结合，赋予防火墙/入侵检测防御系统对新型威胁的检测和拦截能力，采用先放行、再验证的机制，拦截有延迟，无法避免被通报，再到第三代防火墙/入侵检测防御系统+本地威胁情报的方式，基于SDK模式对接，由云端将威胁情报库同步至本地防火墙，毫秒级拦截，风险不出圈，高频率更新半年内威胁情报热数据，充分平衡检测精度与效率。

锐捷入侵检测防御系统产品进化到第三代出站安全防御模式，大容量本地威胁情报库与RG-IDP-P系列入侵检测防御系统的结合，让客户网络边界具备了较强的出站安全检测和阻断能力，本地识别降低了上传云端识别的时间，实时本地检测与阻断。在数据采集上，凭借腾讯安全在云、管、端以及业务侧积累的安全大数据，构建了国内完整的情报数据触点网络，每日处理的原始安全数据可达30000亿条，与锐捷安全团队的生态合作，为用户提供高精准的多种情报，实现精准检测，整体安全能力大幅提升。

全新硬件设计，可靠性更高

针对电压异常、电网异常可能造成存储器件故障的风险，新增相应的监控器件，和备用器件，提升存储器件抗异常冲击的能力，减少设备损坏和数据丢失。

热升级/恢复

秒级热补丁，升级设备运行过程中，可以针对转发组件、管理组件和部分系统组件进行补丁升级并重启相应组件，不影响整机运行，大大提升了设备的可维护性和稳定性。

在设备运行过程中，若转发组件出现突发异常，系统能够实现秒级自动热重启，无需人工介入发现并手动重启设备来恢复，将转发异常的恢复时间从之前的几分钟甚至数小时缩短至几秒钟，大大降低了对用户正常业务转发的影响。

采用全新NTOS操作系统，效率更高

应用业内先进的多核无锁化设计。一般安全设备有多个CPU，工作机理：多个CPU同时从一个公共的内存池中取数据处理，会有多个CPU同时竞争一个数据，获得数据的CPU就会给数据加锁，未获得数据的CPU只能等待解锁再处理，导致效率损失。锐捷新技术：为每一个CPU在内存中划出对应的独立空间，一个CPU就固定从一个内存空间中取数据，不用加锁也不会冲突；数据也按照一定的规律存储，比如同一个IP地址源来的数据都放入同一个内存单元里；这样同一个源地址IP的数据存在同一个内存空间，由同一个CPU处理。TCP/IP一共4层，每一层都采用这种多核无锁化设计，效率提升显著。

业务智能诊断中心

故障分析

RG-IDP-P系列入侵检测防御系统致力于将高级工程师的排查问题能力转化为产品功能，为用户提供一个一站式故障排查向导，按照客户端访问目标资源的路径，自动化执行排查动作，直观呈现故障问题与处置建议，大幅提升排障效率，帮助用户节省排障带来的额外开销。

报文示踪

分析和追踪设备中各个安全业务模块对报文的处理过程，通过查看报文示踪记录的详细信息，有利于管理员对网络故障的快速排查和定位。

端口扫描+流量学习，零基础也能上线

上线配置

RG-IDP-P系列入侵检测防御系统上线配置时，通过“端口扫描”自动识别业务系统IP、端口，再针对性进行“流量学习”自动识别现网业务访问关系，一键生成精细到端口的访问控制策略，零基础也能轻松完成入侵检测系统的上线实施。

服务器端口梳理

日常运维中，为符合更高安全要求，需对服务器端口进行系统梳理，制定更精细化控制策略；传统人工手动做，逐台梳理并与业务方核对，耗时长；现在通过端口扫描+流量学习，1日内完成，不仅大大提高效率，而且一般技术人员也可以胜任。

模拟策略运行，预见调整的效果，策略调整低风险

对策略进行增、删、改的操作，可在模拟空间中，匹配真实流量，分析策略调整前后流量匹配命中的差异，并据此调整策略直至满意。业务不中断也能调策略，彻底告别熬夜调策略的痛苦，把策略调整的风险降至最低，并能实现精细化策略调整。

简易云运维，无需跑现场也能调设备

管理员可以通过锐捷云平台，对入侵检测防御系统进行远程管控，实现设备配置、策略统一下发、设备监控等功能，无需跑现场也能实现设备的日常运维。

04 产品规格

硬件规格

产品型号	RG-IDP-P8600-G20
接口规格	
固化业务接口	16 个 10/100/1000BASE-T 接口 10 个 10GE SFP+ 接口
固化管理接口	1 个 RJ45 的 MGMT 接口 1 个 RJ45 的 Console 接口
USB接口	2个USB 3.0接口
模块插槽	2个扩展模块插槽
系统规格	
硬盘	标配无，支持扩展 1TB HDD/480GB SSD 硬盘
电源与功耗	
电源	支持 2 个可插拔电源模块 RG-NSEC-PA150I，标配无

软件规格

产品型号	RG-IDP-P 系列
网络	
物理接口	支持配置接口为LAN/WAN属性，其中WAN口支持PPPoE、DHCP、静态IP三种模式；支持配置接口为路由、透明和旁路部署模式
路由	支持IPv4，IPv6，静态路由、动态路由、路由策略、策略路由，运营商地址库路由，应用路由等选路策略，出口负载均衡
DHCP服务器	支持DHCP Server功能
DNS服务器/DDNS	支持配置设备的DNS地址；支持多种动态域名解析运营商
对象	
地址/应用/服务	支持设置地址对象、应用类型、服务对象
病毒防护模板	支持设置内容对象模板，提供AV病毒模板，可选择快速查杀模式；可根据协议、方向设置模板；支持设置内容对象模板，提供文件过滤模板（根据文件类型）；支持设置病毒例外
入侵防御模板	支持设置内容对象模板，提供IPS入侵检测模板；支持设置入侵防御模板。可根据对象、严重性、协议、威胁类别设置规则过滤器；支持设置规则例外
URL过滤	支持URL过滤
WEB应用防护规则库	支持对WEB的应用防护规则设置

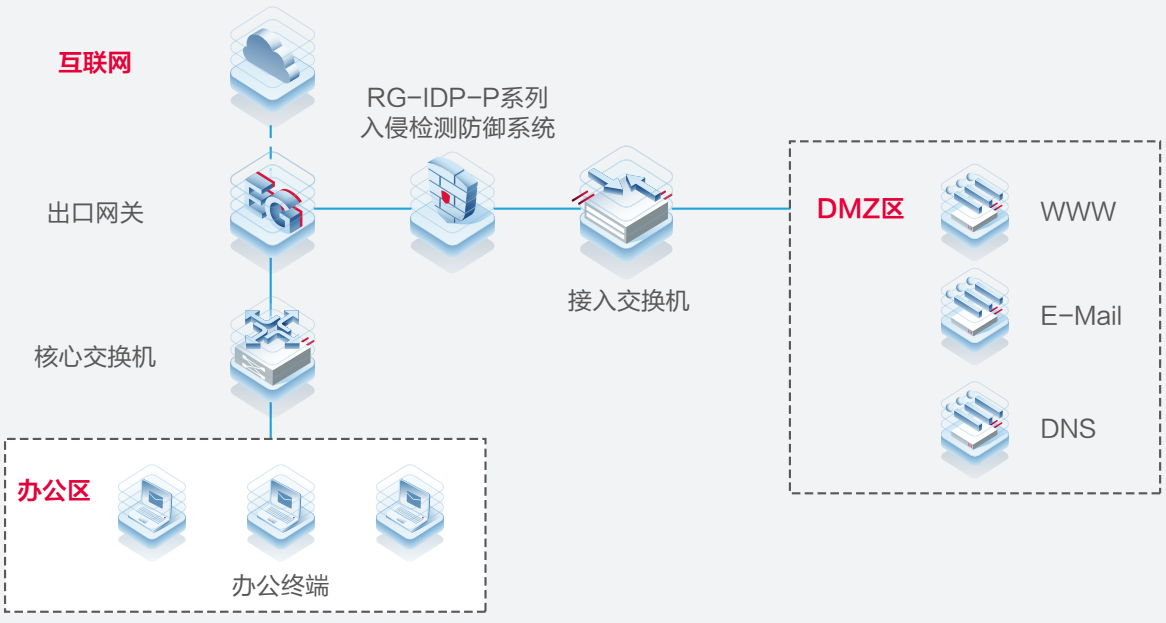
产品型号	RG-IDP-P 系列
用户认证	支持用户管理、用户导入，认证服务器配置、实名同步，配置认证策略
策略	
流量学习	支持流量学习功能，可记录与监控IP相关的IP地址和端口，并可记录异常流量；支持流量学习日志的导出
NAT转换	支持NAT（44/64/46/66）策略，提供NAT地址转换，支持NAT策略的批量导入功能，提供常见的NAT ALG服务，提供服务器端口映射功能，提供NAT地址池状态显示
控制策略	支持控制策略配置，可根据对象、内容、区域等参数来自定义策略，支持策略列表的呈现，支持控制策略的批量导入功能
DoS/DDoS防护	支持安全防护功能，支持各种DDoS防护策略
威胁情报	支持威胁情报功能，可对功能进行开启或关闭，可自定义威胁情报，可管理威胁例外
SSL代理策略	支持设置SSL代理策略。可根据对象、内容、区域等参数来自定义策略，支持策略列表的呈现；支持设置域名白名单、应用白名单；支持配置审计策略、模板、和白名单

05 典型应用

数据中心/园区区域边界安全防护

RG-IDP-P系列入侵检测防御系统可作为数据中心边界/园区区域边界使用，满足网络应用需求、提升信息安全，为核心业务提供安全保障。可以实现以下价值：

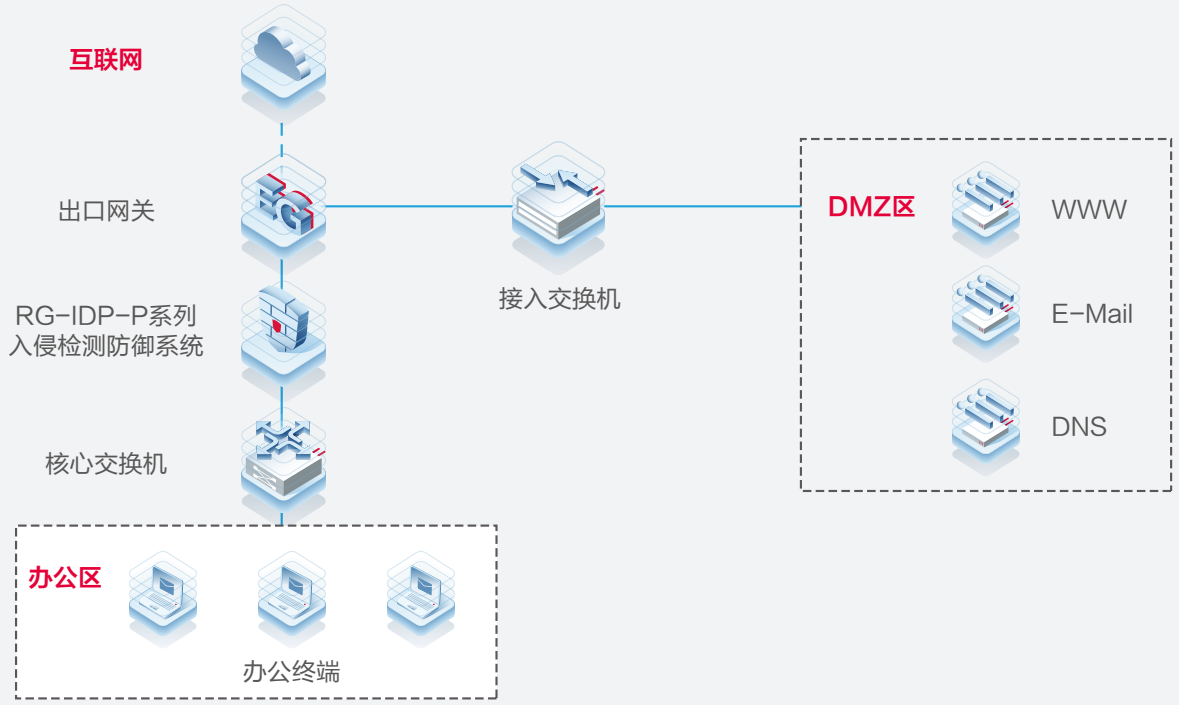
- 针对服务器制定精细化访问控制策略。
- 有效抵御外部攻击，保护企业关键服务。
- 帮助用户进行应用识别、应用控制。



互联网出口

RG-IDP-P系列入侵检测防御系统能够更好的满足互联网出口的需求，提升信息安全，为出口网络提供安全保障。可以实现以下价值：

- 满足互联网出口场景安全防护需求；
- 有效抵御外部攻击，防止病毒等，保护用户关键业务；
- 帮助用户进行应用识别、应用控制。



06 选配指南

RG-IDP-P8600-G20支持通过授权扩展设备性能，硬件也具备良好的可扩展性，支持2个扩展槽，支持2端口40G扩展卡、4 端口万兆光口扩展卡；可扩展冗余电源；可扩展1TB HDD/480G固态硬盘，具体选配信息见7订购信息。

07 订购信息

RG-IDP-P8600-G20

产品型号	产品描述
RG-IDP-P8600-G20	锐捷网络RG-IDP-P系列入侵检测防御系统RG-IDP-P8600-G20，固化16个千兆电口，10个万兆光口，2个接口扩展槽，1U高度，标配无电源，支持扩展热插拔冗余电源，支持扩展硬盘。

产品型号	产品描述
RG-IDP-P8600-G20-1G-LIC	RG-IDP-P8600-G20入侵检测防御系统性能扩展授权，每个授权提供IPS吞吐性能1G扩容，最大可采购6个
RG-IDP-P8600-G20-LIS-1Y	多合一特征库授权，每个授权提供1年病毒库、入侵防御特征库升、应用识别特征库升级服务
RG-IDP-P8600-G20-RTI-LIS-1Y	威胁情报特征库升级授权，每个授权提供1年锐捷联合腾讯威胁情报特征库升级服务
RG-IDP-P8600-G20-RTI-AH-LIS-1Y	威胁情报特征库升级授权，每个授权提供1年锐捷联合安恒威胁情报特征库升级服务
RG-IDP-P8600-G20-URL-LIS-1Y	URL特征库升级授权，每个授权提供1年URL特征库升级服务
RG-IDP-P8600-G20-LIS-E-1Y	多合一特征库授权，每个授权提供1年病毒库、入侵防御特征库升、 URL特征库、应用识别特征库、锐捷联合腾讯威胁情报特征库升级服务
RG-IDP-P8600-G20-LIS-EA-1Y	多合一特征库授权，每个授权提供1年病毒库、入侵防御特征库升、 URL特征库、应用识别特征库、锐捷联合安恒威胁情报特征库升级服务
RG-NSEC-PA150I	冗余电源模块，可按需扩展满足冗余电源的需要

通用辅材

产品型号	产品描述
RG-NSEC-HDD-1T-B	1TB机械硬盘，可按需扩展满足硬盘配置需求
RG-NSEC-2QXS	2端口40G扩展卡
RG-NSEC-SSD-480G-B	480G企业级固态硬盘
RG-BOX-BRACKETS	免锁支架螺丝的设计，能够大幅度提升安装体验及安装速度，挂耳用于保持盒式设备前、后端水平高度一致，防止设备尾端下垂

08 装箱清单

序号	名称	数量	单位
1	主机	1	台
2	固定架	2	个
3	脚垫	4	个
4	固定架安装说明	1	本
5	网络产品保修册及有害物质清单	1	本
6	M4×8 十字槽沉头螺钉 GB819-85	14	个
7	黄绿接地线	1	根
8	后托架	2	个
9	后托架滑轨	2	个

09 保修信息

如需了解产品保修政策和保修期，敬请访问锐捷网站或联系本地销售机构。

- 锐捷保修政策：https://www.ruijie.com.cn/fw/xw/8006/
- 锐捷产品保修期自助查询：https://www.ruijie.com.cn/fw/bx/

说明：实际保修条款依据不同国家/代理商的商业条款决定。

10 更多信息

如需获取更多锐捷相关信息，敬请访问锐捷网站或联系本地销售机构。

- 锐捷网络官方网站：http://www.ruijie.com.cn
- 锐捷网络官方网站服务与支持版块：http://www.ruijie.com.cn/fw/
- 锐捷网络7*24h智能客服闪电兔：http://ocs.ruijie.com.cn
- 锐捷网络7*24h技术服务热线：4008-111-000
- 锐捷网络售后服务工具——小锐云服：http://www.ruijie.com.cn/special/fw/tool/xryf/
- 锐捷网络技术支持与反馈信箱：4008111000@ruijie.com.cn
- 锐捷网络文档支持与反馈信箱：doc@ruijie.com.cn

Ruijie 锐捷
Networks

锐捷网络股份有限公司
欲了解更多信息，欢迎登录www.ruijie.com.cn，咨询电话：400-620-8818