RG-IDP 1000E V2.0

入侵检测防御系统

锐捷网络股份有限公司

了解更多产品信息，欢迎登陆 www.ruijie.com.cn，咨询电话：400-620-8818

产品概述

针对日趋复杂的应用安全威胁和混合型网络攻击，锐捷适时推出了 RG-IDP 入侵检测防御系统以满足用户的安全需求，本产品具备安全实用、高效过滤、检测准确的特点。RG-IDP 产品提供了动态的、深度的、主动的安全防御机制，为企业提供了一个全新的立体的网络安全解决方案。

RG-IDP 入侵检测防御系统是一个深入应用层（七层）的安全设备，主要提供网络威胁防御的业务，不同于交换机、路由器，RG-IDP 本身不参与报文选路和交换，而是透明部署，从一个接口上接收网络流量，对报文进行深入七层的实时分析检测，根据检测结果阻断攻击流量，并将正常流量从另一个确定的接口上转发出去。

产品特性

全面的特征库

RG-IDP 入侵检测防御系统可以帮助用户了解网络的运行状况和发生的安全事件，并根据安全事件来调整安全策略和防护手段，同时改进实时响应和事后恢复的有效性，为定期的安全评估和分析提供依据，从而提高网络安全的整体水平。RG-IDP 内置超过 13000 条签名特征库，全面涵盖恶意活动、漏洞后门、信息侦查、僵木蠕、WEB 攻击、工具利用等威胁类型。

内容安全防护

RG-IDP 入侵检测防御系统能够深入到 HTTP、SMTP、DNS、FTP 等协议对内容进行安全检测及防护，基于关键字识别需要检测的内容，确认不同协议检测位置的内容合法性，并支持正则匹配。

流量自学习

RG-IDP 入侵检测防御系统可以根据资产流量情况，如：TCP 并发连接数量、新建连接速率、带宽、HTTP 请求速率、DNS 查询请求速率、并发 IP 数等多维度进行机器学习，并自动生成限速基线，有效的帮助用户控制流量，缓解网络的资源浪费。

DDoS 防御能力

RG-IDP 入侵检测防御系统能够识别和检测众多的 DDoS 攻击行为，有效防范对网络和主机的扫描攻击、IP 欺骗攻击、源路由攻击、IP 碎片攻击、SYN Flood、Smurf Attack、Ping Of Death、Teardrop Attack、Land Attack、Ping Sweep、Ping Flood、TFN（Tribe Flood Network）等 DoS/DDoS 攻击。

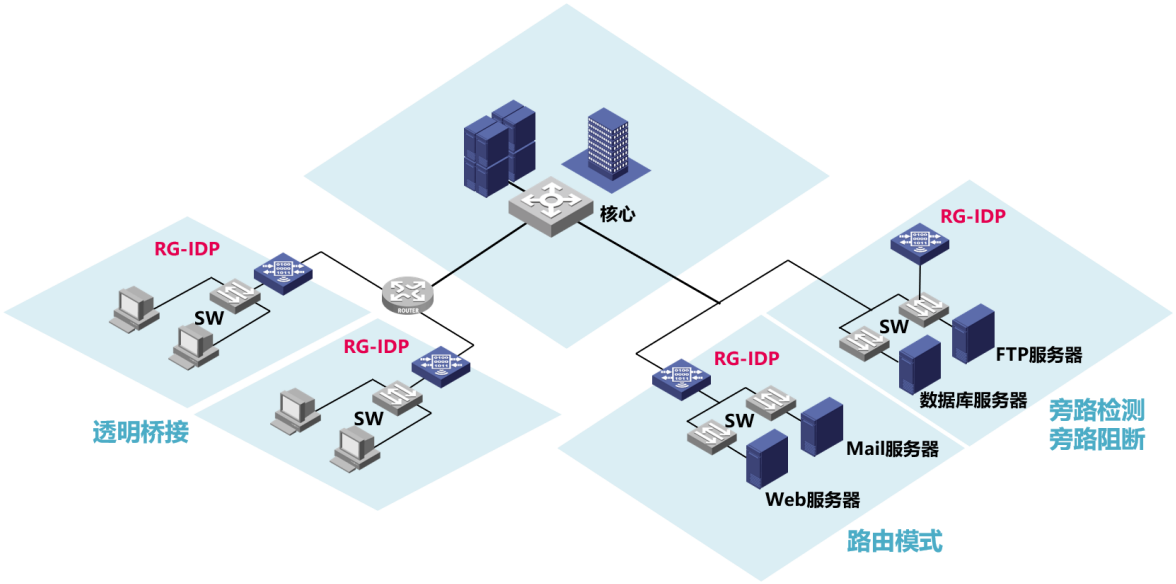
灵活的部署模式

RG-IDP 入侵检测防御系统提供灵活的部署形式：透明模式、路由模式、旁路检测、旁路阻断、双机热备，满足各种用户场景的部署需求。

可视化分析

RG-IDP 入侵检测防御系统在增强产品功能的同时，也同样关注用户的使用感受，可视化资产状态监控、态势感知大屏动态展示、多维度威胁统计、丰富的系统报表，让用户能够清晰的对资产安全状态进行监控。

典型应用



技术参数

产品型号	RG-IDP 1000E V2.0
基本特性	
产品形态	1U
硬件接口	6GE
电源规格	单电源
宽度*深度	430*360
功能参数	
状态监控	系统预览、安全态势、系统状态、连接监控、资产状态、封禁 IP 等基础信息
基础配置	部署模式、防护资产、基础对象、规则库展示
安全防护	入侵防护、DDoS 攻击防护
访问控制	黑白名单、IP 访问控制
外联控制	外联检测
机器学习	流量限速、流量自学习
系统管理	系统配置、授权管理、告警配置、升级管理、备份恢复、运维工具、系统操作、集中管理配置、设备信息上传
网络管理	网络配置、ARP 配置、路由配置
高可用性	HA 管理、端口联动、过载保护、Bypass
日志报表	防护日志、外联日志、审计日志、报表导出、外发配置、日志备份