RG-WG系列

WebGuard

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

随着Web2.0时代的到来，Web已成为社会生活中不可或缺的组成部分。信息获取、网上购物、社交网络、网上银行等Web应用越来越为人们所熟知。伴随着Web应用需求的日益多样化，Web应用的开放性与交互性越来越强，相关的安全问题随之而来，而且呈现日益攀升趋势。据业内报道，Web 应用正成为网络安全盲点。目前黑客攻击所用到的技术都是防火墙、IPS等传统网络安全范畴之外的基于 Web 应用相关的技术手段，如SQL注入、跨站攻击、网站挂马等，很多是利用URL参数，Web交互内容，Web表单输入等Web应用技术达到攻击目的。

因此，IDC托管机房、商业或业务站点、各类Web应用服务器等长期以来一直被Web应用攻击所困扰，随之而来的是客户投诉、虚拟主机用户受牵连、法律纠纷、商业损失等一系列问题。

同时公共信息服务提供者如政府、高校等网站饱受网页篡改、网站挂马等Web攻击的困扰。解决Web应用安全问题已成为当务之急。

RG-WG系列锐捷WebGuard应用保护系统，是锐捷网络专门解决上述Web应用安全问题设计的网络设备。锐捷WebGuard基于对HTTP/HTTPS流量内容的双向检测分析，识别检测各类Web编码、交互技术、URL参数以及表单输入等，为Web应用提供实时、动态的主动性防护。RG-WG系列有三个型号：RG-WG1000EM、RG-WG2000EM和RG-WG 3000EM，分别为不同规模的网络提供Web应用安全解决方案。

锐捷WebGuard，通过对进出Web服务器的HTTP/HTTPS流量相关内容的实时分析检测、过滤，来精确判定并阻止各种Web应用入侵行为，阻断对Web服务器的恶意访问与非法操作，适应Web2.0时代的主动实时监测过滤风险技术，而不是被动的遭受攻击后的恢复，将恶意代码、非授权篡改、应用攻击等众多因素结合在一起进行综合防范，从而做到对Web服务器的多重保护，确保Web应用安全，防止网页内容被篡改，防止网站数据库内容泄露，防止口令被突破，防止系统管理员权限被窃取，防止网站被挂马和植入病毒、恶意代码、间谍软件等，防止用户输入信息的泄露，防止账号失窃，防SQL注入，防XSS攻击等。

产品特性

高性能产品平台

RG-WG系列采用多核硬件架构，优化重写TCP协议栈且支持多核的RGOS，是锐捷WebGuard高性能的技术保障；

并行多核控制器，根据五元组进行会话的识别与数据包的均衡分发，充分发挥多核性能，最高可以实现吞吐量万兆处理性能；

优化重写的用户态TCP Stack，TCP Stack之间处于完全隔离的进程空间，打破了传统Kernel TCP Stack 共享数据锁的限制。

动态网页防护技术

对采用web2.0技术的动态页面，WG提供针对web输入请求的实时检测过滤技术，防御利用动态页面程序设计上所存在的应用安全漏洞而发起的SQL注入、XSS跨站点脚本攻击、缓冲区溢出等攻击，从而防御这些攻击所要达成的目的，包括：绕过登陆身份检查、获得系统管理员密码、非法获取数据、非法篡改数据、生成非法文件、执行非法命令等一系列修改、破坏网站数据库内容、网站架构等的攻击行为，保护web站点内容与服务的安全性与可靠性。

网页防篡改

专门的缓存检测机制，对交付给用户的网页做交付前的检查核实，只有确认合法的网页才能被输出到客户端，被篡改的非法网页将被锁定，不会被访问用户看到，并及时通知管理员进行篡改恢复。

防止网站挂马

能扫描检测URL、URL参数、窗体输入、请求变量、ActiveX、JavaScript、iFrame等；

网站挂马检测引擎，对网站页面进行监控诊断，内置1000多万木马病毒特征库，可自动升级，能及时发现解决WebGuard部署前已被挂马的网站。

Web服务器保护

Web站点系统的隐身保护功能，防止web应用服务器类型、操作系统、数据库、程序源代码等web系统信息的泄露；

保护IDC托管机房、各类商业、业务服务器，保护各类Web服务器如网银、精品课程服务器、游戏服务器、企业ERP系统等。

内置防病毒网关

内置多种Malware检测规则，实时拦截ASP或PHP后门病毒：阻止进而获取Web管理权限的行为。防止网站被挂马，防止Web站点成为Malware发布源头：避免遭受名誉损失和客户商业损失；

防御包含病毒木马的自动化攻击。减轻管理员服务器例行杀毒工作量，有效防御网站攻击。

WebShell侦测与阻断

实时检查过滤webshell攻击的命令，阻止入侵者访问调用webshell文件；

阻止利用webshell发起的各种攻击或入侵行为：挂马、注入、文件下载、内容篡改等。

Web加速功能

WG可以配置为WEB加速模式，对WEB服务器的静态页面内容进行Cache，客户端对这类页面的访问可以直接通过WAF缓存中获取，避免了用户重复通过Web服务器并进行协议解析等相关操作，从而加快了访问速度，减轻了WEB服务器的负担。

Cookie保护

通过对Cookie内容的加密来防止Cookie明文传输所造成的内容泄露；

通过针对Cookie内容的校验，达到防止Cookie内容被篡改；

通过同时校验Cookie内容和客户端IP的方式，防止Cookie被劫持。

关键字过滤

内容关键字过滤，避免网站被上传反动、暴力、色情等类型关键字内容，影响社会和谐，支持中英文关键字；

协议关键字过滤，允许用户自定义关键字内容，为个性化业务系统定制特色保护功能。

完善的黑白名单功能

动态攻击黑名单。RG-WG系列能将确认为攻击的源IP自动加入黑名单，并且提供自动解禁时间，不需要任何人工的操作，大大方便了管理员的维护与管理；

RG-WG系列能定制网站管理页面的访问IP，杜绝非网站管理员访问网站管理页面，从而预防攻击者直接修改网站页面；

支持基于IP、域名、URL的黑白名单。

合规性检查

满足网页防篡改合规性检查需求；

既能对事后恢复，又能事前保护，防御合规性检查的探测攻击。

丰富的访问报表

RG-WG系列提供丰富的Web服务器访问日志与报表，提供病毒检测日志与报表，Web攻击检测防御日志与报表，还提供设备运行情况和负载的统计图表，不仅方便管理员对Web服务器的运维，还方便管理员对WebGuard本身的运维；

通过WebGuard的访问报表，管理员可以掌握网站由谁访问，以及攻击者物理位置，从而有针对性的对网站进行改进。

支持多站点管理员

RG-WG支持多web网站管理员独立配置各自的站点策略管理，且有独立的日志与报表；

支持基于服务器IP及IP段/IP列表的安全策略；支持基于URL的安全策略。

易部署

RG-WG系列支持免配置初次运行，如果用户并非安全专家，默认配置即可防范大多数攻击；

内置多种攻击防御模型，根据Web交互内容识别匹配应用逻辑定位攻击，与服务器本身并无关联。轻松实现对web站点的默认防护，可根据不同的站点防护需求，制定不同的防护规则。

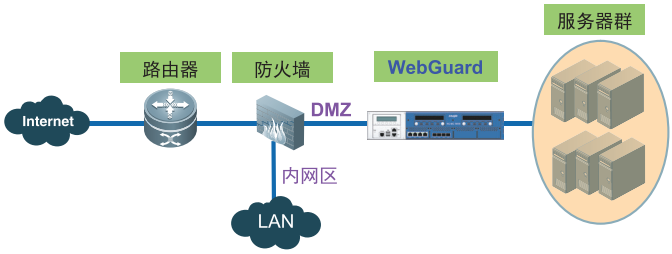
技术参数

产品型号	RG-WG 3000EM	RG-WG 2000EM	RG-WG 1000EM
Console接口	1	1	1
大小	2U高度 19"标准机柜	2U高度 19"标准机柜	1U高度 19"标准机柜
电源输入	100-240VAC 60-50Hz/8-5A	100-240VAC 60-50Hz/8-5A	100-240VAC 60-50Hz/8-5A
湿度	5-95% RH	5-95% RH	5-95% RH
工作温度	0℃-50℃	5℃-35℃	0℃-40℃
软件旁路	支持	支持	支持

典型应用

部署一：服务器区集中式部署

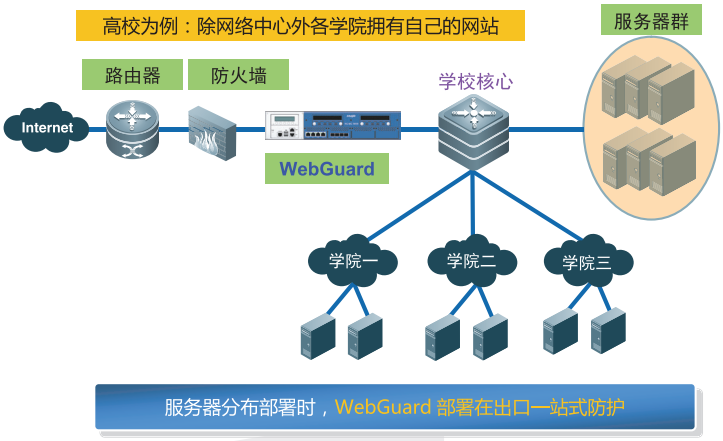
当待保护Web服务器集中部署，服务器区统一出口时，可以将WebGuard部署在服务器区。



当服务器集中部署，统一出口时，WebGuard 部署在服务器区

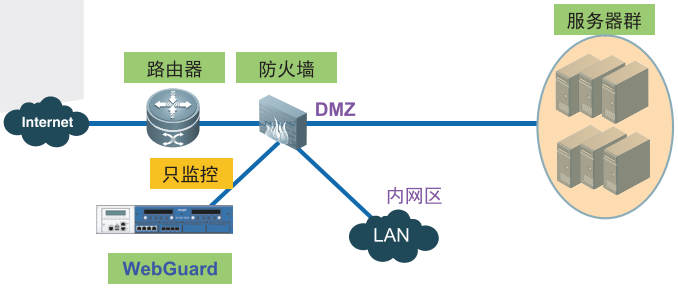
部署二：服务器分布部署，WebGuard出口一站式防护

当Web应用系统多网段分布部署时，WebGuard部署在出口，提供集中一站式的防护。以高校为例，某高校，具有多个专业学院，每个学院甚至每个系具有分布部署的多个Web服务系统，通过在该高校出口处部署一台WebGuard产品，就能达到对全部Web应用服务器的防护，使投资回报率最大化。



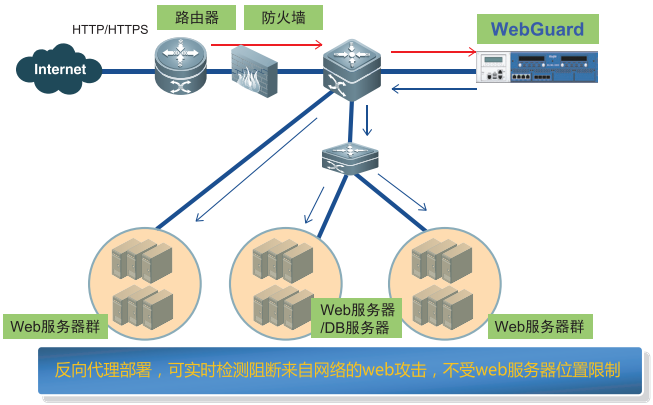
服务器分布部署时，WebGuard 部署在出口一站式防护

部署三：旁挂部署，只做监控



初次部署时，建议先旁挂监控，待全面掌握网络情况后，再在线部署

部署四：反向代理模式，物理旁路，逻辑串联



订购信息

型 号	描 述
RG-WG 3000EM	高端万兆WebGuard应用保护系统
RG-WG 2000EM	高端千兆WebGuard应用保护系统
RG-WG 1000EM	高端百兆WebGuard应用保护系统
RG-SEC-4SFP	4千兆光口扩展卡
RG-SEC-8GE	8千兆电口扩展卡
RG-SEC-8SFP	8千兆光口扩展卡
RG-SEC-4GE4SFP	4千兆光加4千兆电口扩展卡
RG-SEC-2XEF	2口SFP+万兆光模块
RG-WG 1000EM-LIS-1Y	RG-WG 1000EM应用特征库授权1年
RG-WG 2000EM-LIS-1Y	RG-WG 2000EM应用特征库授权1年
RG-WG 3000EM-LIS-1Y	RG-WG 3000EM应用特征库授权1年

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