速龙软件

优秀的网站服务器安全防护方案

速龙网站智能自动防护系统

北京速龙软件科技有限公司

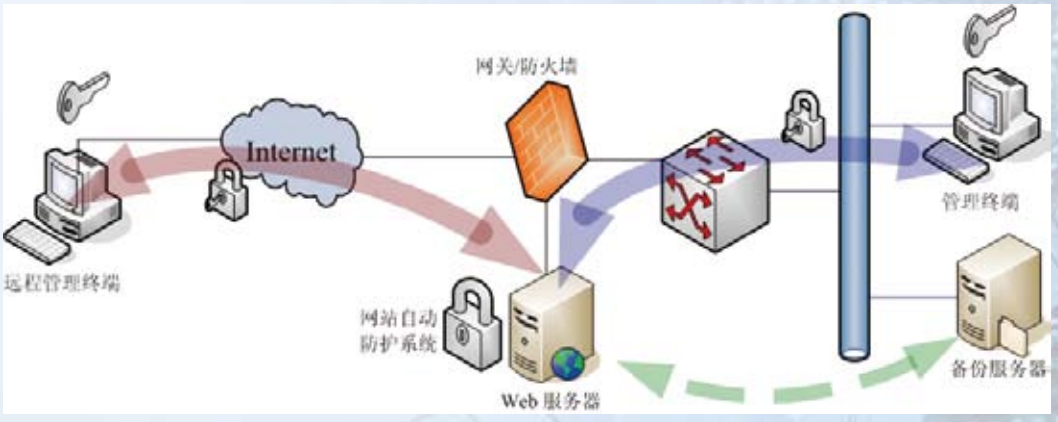
概 览

您的服务器在24小时不间断的提供着服务，可是病毒、木马、攻击行为是如此之多，时刻窥伺着您的服务器，如何为它提供24小时不间断的保护？

据近两年权威统计资料数据显示，安全事件中超过50%是非法篡改、删除、窃取主机内文件、数据、资料的行为。即便是防范严密的系统，部署了IDS、防病毒软件和防火墙，攻击行为仍然不请自来，令人防不胜防。我们推出的 “速龙网站智能自动防护系统”，围绕网站服务器的文件保护，提供了“防护+管理应用”的完整解决方案。

该系统由网站服务器保护系统、备份系统、管理员本地及远程控制台系统组成。主要用于阻止对网站服务器中受保护文件的非授权改动，可以保护网站服务器中的任何格式的文件，并且能侦测与阻止SQL注入攻击，该产品与防毒系统、防火墙、入侵检测系统结合在一起，共同提供完整的网站服务器安全解决方案。

“速龙网站智能自动防护系统”中的文件系统保护功能将底层驱动、文件特征码高速扫描比对、应用程序授权等方式结合在一起，为网站服务器中受保护的文件系统提供了极为严密、低系统负载的保护；SQL注入防护功能采取语法分析与表达式计算的方法，摒除简单过滤关键词所带来的处理不完整、防护不严密的缺点，能有效的阻止SQL注入攻击，即便网站的代码本身并没有任何针对SQL注入攻击的处理，“速龙网站智能自动防护系统”中的SQL注入防护模块也一样能有效的阻止SQL注入攻击。



系统使用与网上银行同等安全级别的USB Key进行系统本身的授权、管理和通信。提供了有效的安全保障。

适用对象

政府网站、企事业单位网站、ISP、IDC等服务器租赁托管服务商、企业内部OA网络、ERP、CRM等业务服务器。

系统组成

整个系统由服务器保护系统、备份系统、管理员本地及远程控制台系统组成。其中服务器保护系统又包括了文件保护模块和SQL注入攻击防护模块。

系统功能

文件保护服务

由管理员将网站的发布目录或者其他需要保护的目录设置为保护状态，设置了保护以后的文件目录中的文件、子目录只能由授权程序改动，除此以外的进程都无法对受保护的文件目录下的内容进行修改，即便攻击者攻破了防火墙、获取了操作系统的管理员权限，仍然无法对受保护的目录下的文件进行改动。服务器控制台程序通过USB Key，使用独立的身份认证系统进行授权认证，因此即便系统的其他安全防护措施遭到攻破，“速龙网站智能自动防护系统”依然能有效地作为最后一道保护屏障。

◆ 文件备份服务

系统提供了自动备份功能，服务器上的受保护目录中的内容被自动备份到备份服务器上，对于授权用户进行的文件改动，将自动同步更新到备份服务器，这样就提供了一个更为稳妥的保障。文件备份过程采用1024位的数字证书加密。

◆ 文件恢复服务

如果受保护目录下的文件、子目录被非授权更改，文件恢复服务将自动从备份服务器予以恢复。文件恢复过程采用1024位的数字证书加密。

◆ SQL注入防护

针对Web服务器的SQL注入攻击是最常见的攻击手段之一，通常情况下网站程序员采取关键词过滤等方法防止SQL注入攻击，但是很多SQL注入攻击是采取单纯的关键词过滤无法防范的。在“速龙网站智能自动防护系统”中，采用了词法分析、表达式分析、计算、关键词过滤等手段，对于客户端提交的HTTP数据，进行高效的分析与计算，寻找其中可能存在的SQL注入企图，并按照系统设置的策略予以处理，所能处理的包括SQL注入、Blind SQL注入、XSS攻击、文件注入攻击、Command 注入、Coldfusion注入、SSI注入、PHP注入等等。

◆ 报警服务

一旦检测到文件攻击、SQL注入攻击等行为，即可按照管理员设置的报警周期、报警方式报警，目前支持的报警方式包括邮件报警与短信报警。

◆ 日志审计

针对文件防护、文件恢复、SQL注入攻击、远程管理、报警信息等方面提供详细的可审计日志，管理员可对日志进行排序、分类、输出等操作。

◆ 远程集中管理

管理员可以在服务器上颁发远程管理授权USB Key，然后使用该USB Key通过远程方式对服务器进行集中式的设置和管理。其中的通信采用1024位的数字证书进行加密。

● 功能一览表

功 能	
保护静态网页文件	支 持
保护动态脚本程序文件	支 持
保护图片、文本及其他附属文件	支 持
防范连续篡改攻击	支 持
授权应用程序白名单	支 持
远程集中管理	支 持
远程维护文件	支 持
受保护文件自动备份	支 持
SQL注入攻击防范	支 持
报警功能	支 持
审计日志	支 持

★ 系统特点

◆ 资源占用低

所采用的文件保护模块以及SQL注入防护模块，均尽可能在算法上进行优化，使系统负载的增加降到最低，根据实际测试，对于日Pageviews为10万次左右的网站服务器，对于CPU平均负载和用户响应时间的影响不超过2%。

◆ 防护严密

系统提供的文件保护功能，即便服务器被黑客或者非授权人员操控，只要服务器控制台模块没有被控制，就无法对受保护的文件夹下的内容进行修改，如果通过远程访问的方式，则困难更大；即便出现了受保护文件遭到非法篡改的情况，文件恢复服务也将自动从备份服务器用最后备份的文件进行恢复。另外，系统所提供的SQL注入攻击防护模块，也采用了高效的语法分析、表达式分析与计算模块，能非常有效的防止SQL注入攻击。

◆ 银行级安全性

系统采用网银级别的USB Key用于自身的授权体系，管理员、远程管理员的帐号密码采用独立的身份管理认证体系进行管理，只有持有授权USB Key的操作人员在验证了所持USB Key密码的情况下才能对系统进行操作和管理；通信方面，采用1024位的加密算法，其中的加密钥匙由管理员随机生成。

◆ 完整的全套应用方案

- **灵活的用户管理**　管理员可以增加或删除普通用户，普通用户仅具备文件操作、文件备份的功能，这样一些日常工作可以由普通用户来完成。普通用户的资料亦存储在管理员USB Key中。
- **便捷的远程管理**　系统提供管理员远程控制台程序，通过该控制台程序，管理员可以在远程对服务器进行设置与管理。采用基于1024位密钥的SSL通信，远程管理可以安全的进行而无需担心中途被截获或篡改。
- **远程文件维护**　管理员可以授权用户通过远程方式对授权目录进行更新等操作，对于ISP等主机托管和虚拟主机服务商尤其方便。
- **文件自动备份**　系统提供了自动备份与恢复服务，对受保护文件夹进行自动增量备份，增加更多一份的安全保障。
- **完备的日志**　系统记录了完整的日志，通过对这些日志，管理员可以进行有针对性的管理，并可在适当的时候作为司法证据。

◆ 部署简单，使用方便

无需改变现有网络结构，安装部署和使用均非常简便。

运行环境

● 软件环境

	备份服务器	服务器	管理员远程控制台
操作系统	Microsoft Windows 2000 Server、Professional系列、2003 Server、Windows XP		
Web服务	N/A	IIS	N/A
SQL注入防护		IIS 5.0/IIS 6.0	
其 他	TCP/IP网络环境		

● 硬件环境

备份服务器	服务器	管理员远程控制台
CPU：PII 400及以上 内存：512M及以上 硬盘剩余空间：1G 及以上	CPU：PII 400及以上 内存：512M及以上 硬盘剩余空间：1G 及以上	CPU： PII 400及以上 内存： 128M及以上 硬盘空间：10M及以上

北京速龙软件科技有限公司

网址：www.slsoft.com.cn

地址：北京市西城区黄寺大街26号院德胜置业大厦1号楼607

电话：010-82809450/62/92

传真：010-82809490

指定经销商