



## 目录

前言.....	1
1、序言.....	1
2、关于手册.....	1
3、关于本产品.....	2
4、关于售后服务.....	2
第一章 安装风云	
1.1 安装程序.....	4
1.2 验证产品.....	7
1.3 卸载产品.....	7
第二章 设置风云	
2.1 系统设置.....	9
2.2 网络防火墙设置.....	10
2.2.1 端口过滤设置.....	10
2.2.2 IP 地址过滤设置.....	11
2.2.3 抗 DDOS 攻击设置.....	11
2.2.4 ARP 防护设置.....	12
2.2.5 SQL 防注入设置.....	13
2.3 主动防御系统设置.....	13
2.3.1 进程保护设置.....	13
2.3.2 文件保护设置.....	14
2.3.3 注册表保护设置.....	15
2.3.4 系统用户名监控设置.....	16
第三章 功能说明	
3.1 防入侵功能.....	18
3.2 防 DDOS 攻击功能.....	20
3.3 后台管理功能.....	20
3.4 远程设置功能.....	21
3.5 短信通知功能.....	21
附录.....	26



## 前 言

### 1、序言

感谢您购买和使用风云防火墙服务器入侵防御系统，现在您的服务器已经拥有了风云全方位的保护，风云防火墙服务器入侵防御系统是基于网络数据包过滤和“主动防御”技术开发的新一代服务器安全产品，该产品抗 SYN 和 CC 类 DDOS 攻击和防 SQL 注入入侵等功能均采取易用式操作界面，让您轻点鼠标就可以实现外抗攻击、内保安全的双重保护。

### 2、关于手册

本手册由各个章节组成，详述和解释了风云防火墙服务器入侵防御系统的许多特性、选项、用法说明、术语以及该软件的其它重要技术信息。

本手册是针对初用本产品的网站管理人员。手册不是要教您关于某个功能或者设置的全部内容，而是陈述并讨论本产品的各种特性，并逐步引导您熟悉网站安全知识和灵活配置本产品的办法。

风云防火墙服务器入侵防御系统是一款基于网络数据包过滤和“主动防御”技术开发的新一代服务器安全产品，能有效抵御各类 DDOS 攻击和防止网站被入侵，但是由于各种服务器性能的不同和网站管理员的不同需求，您需要花点



时间来学习和理解本产品是如何工作的，以使本产品更好的为您服务，不论您的经验如何，您都可以从本手册和我们的技术人员那里获得帮助信息，我们非常乐意为用户解决一切关于网站安全的相关问题。

### 3、关于本产品

风云防火墙是安徽天达网络科技有限公司自主研发的网络安全软件产品，2009年经过《公安部信息安全产品检测中心》、《公安部计算机信息系统安全产品质量监督检验中心》等部门检测合格并符合防入侵产品安全功能要求（GA/T 696-2007），并获得《公安部公共信息网络安全监察局》颁发的《计算机信息系统安全专用产品销售许可证》，安徽天达网络科技有限公司对该软件拥有独立的知识产权，受中华人民共和国版权法及国际版权条约和其他知识产权法及条约的保护，任何单位和个人未经允许复制和销售本产品将被视为违法侵权行为，安徽天达网络科技有限公司将保留追究权利并在适当时候以诉讼的方式解决。

### 4、关于售后服务

风云的售后服务部门是由经过专业培训的技术人员组成，他们能跟踪和解决用户可能遇到的各种问题。风云一直致力于打造安全的网络环境，我们深深地知道及时高效的技术支持的重要性。因此，所有的正版软件用户将得到免费的技术支持和产品的维护更新。



全国免费服务热线: 400-662-2218

传真: 400-662-2218 分机 2

E-mail: kefu@218.cc

官方网站: <http://www.218.cc>

公司名称: 安徽天达网络科技有限公司

公司地址: 安徽省合肥市高新区软件园 2 号楼 314#

邮编: 230088

公司电话: 0551-5318577



## 第一章 安装风云

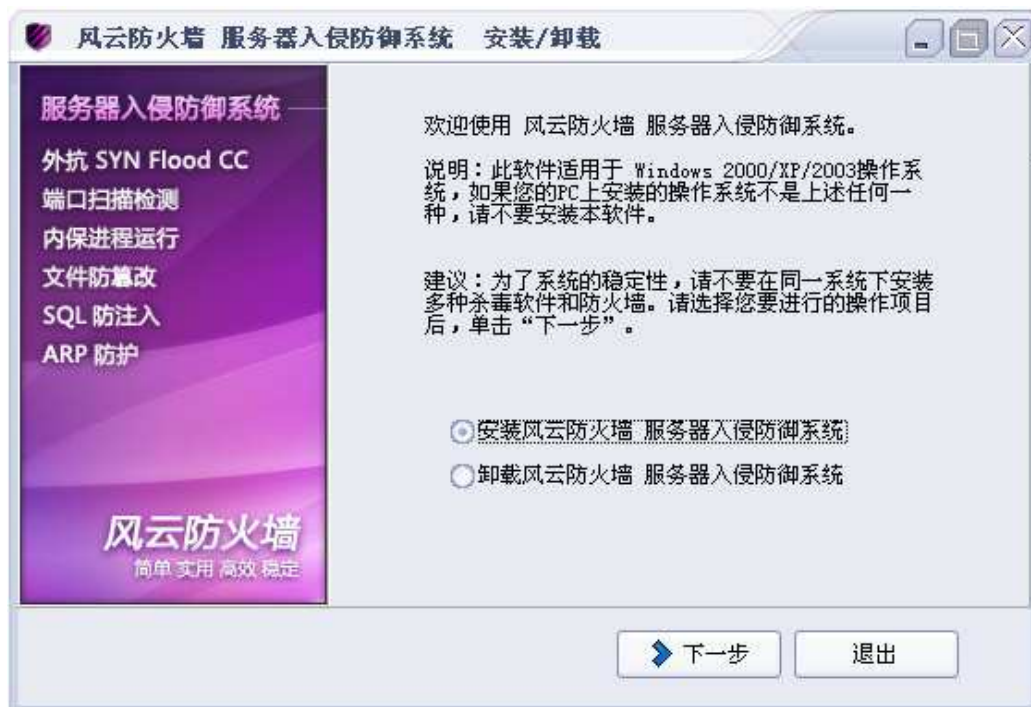
### 1.1 安装程序

由于风云防火墙服务器入侵防御系统在安装时默认您的服务器所有程序都是安全的，所以请在确保服务器安全的情况下安装风云，我们强烈建议您在安装完操作系统后立即安装风云防火墙服务器入侵防御系统，并到我们的官方网站（<http://www.218.cc>）注册为会员。



FYSetup.exe

双击风云安装包文件，将出现以下界面



直接点击“下一步”将出现《软件许可协议》协议界面：



请仔细阅读后选中“本人同意并接受《软件许可协议》”点击“下一步”进入程序安装目录设置页面



我们建议您将程序安装在默认目录下, 点击下一步后进入



## 安装设置界面



设置完成后点击下一步



请在以上界面中输入序列号（序列号为一串五组五位字符，



请在光盘包装上查找) 以及您在我们网站注册的会员帐号, 以便我们提供更加优质的服务。点击下一步后程序完成并提示重启操作系统, 重启后风云安装完毕。


## 1.2 验证产品

打开风云服务器后台管理中心 (<http://www.218.cc/buypro.php>), 登陆后点击“服务器绑定”操作, 输入相应的产品序列号、服务器 IP 地址和您的手机号码等信息, 点击确定。(注: 一个用户名可以购买和绑定多个产品)

产品名称	购买时间	绑定时间	到期时间	状态	功能
风云服务器版 [66-8]	2009-10-06	2009-10-06	2010-10-06	正常	序列号 续费 修改 管理
风云服务器版 [66-3]	2009-09-21	2009-09-21	2010-09-21	正常	序列号 续费 修改 管理
风云服务器版 [66-7]	2009-08-24	2009-08-24	2010-08-24	正常	序列号 续费 修改 管理
风云个人版	2009-08-23	2009-08-23	2010-08-23	正常	序列号 续费

绑定成功后, 您就可以通过该后台管理中心来管理您的产品, 如果您输入了手机号码, 我们会及时将您服务器的相关状态发送到您的手机上, 让您随时随地掌握服务器动态。

## 1.3 卸载产品

如果您不需要风云或者有必要将其删除时, 请运行开始菜单中  卸载风云防火墙-[服务器入侵防御系统] 将出现以下界面, 点击“是(Y)”, 系统重启后风云防火墙将彻底被卸载。





## 第二章 设置风云

程序安装完成后，请确保重启操作系统后再进行程序设置，我们为您进行了一般网站服务器的常规设置，并默认将您服务器中当前所有程序设置为安全。

### 2.1 系统设置

首先，我们需要对风云进行总体的设置，点击风云主界面右侧的系统配置，

风云防火墙

www.218.cc 我们为您保驾护航!

风云防火墙  
简单 实用 高效 稳定

网络防火墙

端口过滤

IP地址过滤

抗DDOS攻击

ARP 防护

SQL防注入

主动防御系统

**基本状态**

项目	总数	已拦截	速度
接收 ICMP	25	24	0
发送 ICMP	0	0	0
接收 UDP	31144	0	0
发送 UDP	31092	0	0
接收 TCP SYN	28	0	0
发送 TCP SYN	115	0	0
接收 ARP Request	119	0	0
接收 ARP Reply	16	0	0
发送 ARP Request	6	0	0
发送 ARP Reply	0	0	0

**监控状态**

- SYN 抗攻击状态  已启用
- ARP 防火墙状态  已启用
- 进程保护项状态  学习模式
- 文件保护项状态  规则模式
- 注册表保护状态  放行模式

**系统配置** **程序日志**

**流量统计**

最大接收速度: 3.72 KB  
当前接收速度: 0.00 B  
001:05:43 22:10 22:08 22:05  
最大发送速度: 922.00 B  
当前发送速度: 0.00 B

接收数据: 15.21 MB  
发送数据: 4.54 MB

进入系统配置页面，在此页中，请将您需要的功能选项选中，并正确输入用户名和各类密码，点击保存应用后请妥善保存您的密码，它将是您开启风云和远程配置风云以及享受官方



售后服务的凭证。



## 2.2 网络防火墙设置

### 2.2.1 端口过滤设置





点击“网络防火墙”中的端口过滤按钮进入设置界面：默认状态下允许所有端口访问，您可以根据服务器的具体情况在右侧表单内填入端口号设置允许或拦截的 TCP 端口或 UDP 端口。

### 2.2.2 IP 地址过滤设置



点击“网络防火墙”中的“IP 地址过滤”按钮后进入 IP 地址过滤设置界面，在底部表单中输入您要拦截或者允许的 IP 地址并点击“添加 IP”按钮将其增加到系统规则中。

### 2.2.3 抗 DDOS 攻击设置

点击“网络防火墙”中的“抗 DDOS 攻击”按钮后进入抗 DDOS 攻击设置界面，根据您服务器的具体情况设置需要开启的防护功能和填写相关数字，我们经过详细的调研和分



析，综合目前各大网站受攻击的情况，已经为您设置好了默认规则，如果您的服务器没有特殊要求，我们建议您不要修改此栏目下的配置，或者在我们的技术人员的指导下进行设置。

### 2.2.4 ARP 防护设置





点击“网络防火墙”中的“ARP 防护”按钮后进入 ARP 防护设置界面，如果你的服务器经常出现 IP 冲突或者掉线的情况，请及时开启 ARP 防火墙，并选中“启用 IP 冲突保护”和“启动 ARP 事件日志”等功能。

## 2.2.5 SQL 防注入设置



点击“网络防火墙”中的“SQL 防注入”按钮后进入 SQL 防注入设置界面，在“指定 HTTP 端口”中添加您网站的 WEB 端口，多个端口请全部添加进去，选中相关防护策略后进入下一步主动防御系统设置。

## 2.3 主动防御系统设置

### 2.3.1 进程保护设置



点击“主动防御系统”中的“进程保护”按钮后进入进程保护设置界面，安装刚完成时系统处在学习模式，此时系统会自动导入您当前系统中的所有进程，并默认放行，当您不允许其他程序运行时，请选中“默认拦截模式”，如果您有特殊程序需要操作所有进程，可通过点击“可运行所有进程白名单”来添加程序，添加完毕后请确保选中“默认拦截模式”，自此之后，防火墙将不允许“进程保护规则”列表以外的任何程序运行，“进程保护规则”列表中所列进程将按照您设置的“启动规则”管理。如果您在“发短信”中设置了“是”，则系统尝试启动该进程时会发送短信到您在风云后台管理中心所填的手机号码中。

### 2.3.2 文件保护设置



点击“主动防御系统”中的“文件保护”按钮后进入文件保护设置界面，文件保护设置与进程保护设置类似，安装刚完成后程序处在放行模式，请在添加相应规则后选中“文件保护规则模式”，并可根据需要具体设置文件或者文件夹的“新建”、“删除”、“重命名”、“修改”、“是否发送日志到服务器”、“是否发送短信到手机”等属性，风云将按照您设置的保护规则对文件进行处理，如果你有特殊的程序需要操作“文件保护规则”列表中的文件，可点击“添加特权程序”进行设置。

### 2.3.3 注册表保护设置



点击“主动防御系统”中的“注册表保护”按钮后进入注册表保护设置界面，注册表保护设置与文件保护设置类似，安装刚完成后程序处在放行模式，请在添加相应规则后选中“注册表保护规则模式”，并可根据需要具体设置注册表的“路径”、“键名”、“新建项”、“新建和修改值”、“删除值”、“是否发送日志到服务器”、“是否发送短信到手机”等属性，风云将按照您设置的保护规则对注册表进行保护，如果您有特殊的程序需要操作“注册表保护规则”列表中的注册表项，可点击“添加特权程序”进行设置。

#### 2.3.4 系统用户名监控设置



点击“主动防御系统”中的“系统用户名监控”按钮后进入系统用户名监控设置界面，点击刷新应用，“现有用户名列表”中将会列出当前系统中所有用户名，您根据需要决定是否选中右侧功能对话框。常规下，系统新增了帐户名，表明服务器被入侵的可能性较大，我们建议您将“启动帐户监控功能”、“发现新增帐户发送短信通知”、“发现新增帐户直接删除”、“监控事件提交网络日志”四项全部选中。

如果您需要监控远程桌面登陆服务器情况，就可以选中“用户登陆系统事件短信通知”，并设置好远程桌面端口后点“应用”按钮即可。如果启用了网络日志，登陆情况也会提交到网络日志服务器保存，如下图（对于多人管理一台服务器，登陆监控日志是一项很有用的功能，方便查询登陆服



务器情况，对分析入侵行为有很大的帮助）：

服务器重启登陆记录

61.191. [redacted] [redacted]

提交时间	服务器信息	服务器IP
<input type="checkbox"/> 2009-11-06 10:06:31	2009-11-06 10:06:31 用户[Administrator]注销登陆. 端口:3389 IP:61.132. [redacted] <安徽省合肥市 电信>	61.191. [redacted]
<input type="checkbox"/> 2009-11-05 16:05:37	2009-11-05 16:05:37 用户[Administrator]登陆系统. 端口:3389 IP:61.191. [redacted] <安徽省铜陵市 电信>	61.191. [redacted]
<input type="checkbox"/> 2009-11-04 17:55:08	2009-11-04 17:55:08 用户[Administrator]注销登陆. 端口:3389 IP:121.23. [redacted] <河北省廊坊市 联通>	61.191. [redacted]
<input type="checkbox"/> 2009-11-04 17:54:43	2009-11-04 17:54:43 用户[Administrator]解锁登陆. 端口:3389 IP:121.23. [redacted] <河北省廊坊市 联通>	61.191. [redacted]

至此，您的风云已经基本设置完毕，您的服务器已处在风云严密的保护之下，值得一提的是，如果你的服务器中有多个网站或者安装了虚拟机系统，只需安装一套风云防火墙服务器入侵防御系统即可。



## 第三章 功能说明

### 3.1 防入侵功能

风云通过详细的安全策略设置和独创的智能判断防入侵机制、简单易用的操作界面，使用户轻松点击鼠标就能保护服务器中所有网站不被入侵，而不需频繁升级您的网站程序。

**端口扫描检测：**当入侵者尝试扫描您网站服务器的端口时，风云通过智能判断后会立即屏蔽入侵者的 IP 地址，把入侵者从一开始就拒之门外。

**SQL 防注入：**SQL 注入是指通过 SQL 命令插入到 Web 表单递交或输入域名或页面请求的查询字符串，最终达到欺骗服务器执行恶意的 SQL 命令，实现入侵网站的目的，SQL 注入是目前互联网上最为流行的入侵网站方式之一，而风云通过严格的字符过滤快速分辨出注入连接并将其屏蔽，详细的分离式网络日志存储功能将每一个尝试入侵者的 IP 地址提交到官方网站后台存储，除了能防止您的网站被入侵，更能为维护网络安全、打击黑客犯罪提供强有力的支持。

**智能主动防御：**进程保护、文件保护、注册表保护等功能，让任何未经授权的程序都无法运行，入侵者即使通过其他方式上传了恶意程序，也无法对服务器实施任何破坏。



时间	父进程	目标进程	操作	当前进程用户
2009-10-24 14:52:07	C:\WINDOWS\explorer.exe	C:\WINDOWS\system32\snd...	拦截	WWW-F311EA7FAP6-...
2009-10-24 14:52:03	C:\WINDOWS\explorer.exe	C:\WINDOWS\system32\snd...	拦截	WWW-F311EA7FAP6-...
2009-10-24 14:51:47	C:\WINDOWS\explorer.exe	C:\Program Files\Intern...	拦截	WWW-F311EA7FAP6-...
2009-10-24 14:51:44	C:\Program Files\Kasper...	C:\Program Files\Kasper...	放行	NT AUTHORITY-SYSTEM
2009-10-24 14:51:26	C:\WINDOWS\system32\w...	C:\Program Files\Lenovo...	拦截	NT AUTHORITY-SYSTEM
2009-10-24 14:50:56	C:\WINDOWS\system32\w...	C:\WINDOWS\system32\log...	放行	NT AUTHORITY-SYSTEM
2009-10-24 14:50:55	C:\WINDOWS\system32\w...	C:\WINDOWS\system32\run...	放行	NT AUTHORITY-SYSTEM
2009-10-24 03:51:47	C:\WINDOWS\system32\w...	C:\WINDOWS\system32\log...	放行	NT AUTHORITY-SYSTEM
2009-10-24 03:35:01	C:\WINDOWS\explorer.exe	C:\Program Files\FYSafe...	放行	WWW-F311EA7FAP6-...
2009-10-24 03:32:20	C:\WINDOWS\explorer.exe	C:\Program Files\FYSafe...	拦截	WWW-F311EA7FAP6-...
2009-10-24 03:32:03	C:\Program Files\FYSa...	C:\Program Files\FYSafe...	拦截	WWW-F311EA7FAP6-...
2009-10-24 03:32:03	C:\Program Files\FYSa...	C:\Program Files\FYSafe...	拦截	WWW-F311EA7FAP6-...
2009-10-24 03:31:59	C:\Program Files\FYSa...	C:\Program Files\FYSafe...	拦截	WWW-F311EA7FAP6-...
2009-10-24 03:31:59	C:\Program Files\FYSa...	C:\Program Files\FYSafe...	拦截	WWW-F311EA7FAP6-...
2009-10-24 03:31:59	C:\Program Files\FYSa...	C:\Program Files\FYSafe...	拦截	WWW-F311EA7FAP6-...
2009-10-24 03:31:31	C:\Program Files\FYSa...	C:\Program Files\FYSafe...	拦截	WWW-F311EA7FAP6-...

### 3.2 防 DDOS 攻击功能

风云防火墙服务器入侵防御系统能有效抵御 SYN 类和 CC 类洪水攻击，确保服务器在被攻击状态下的正常运行，并能记录 CC 类洪水攻击的来源 IP 地址，风云强有力的售后服务和技术支持将协助您尽力找出攻击者。

### 3.3 后台管理功能

用户登陆 <http://service.218.cc/buypro.php> 风云后台管理网站，即可详细查阅您的服务器各类日志，了解服务器运行状态和历史记录，为您正确评估服务器安全风险提供依据。并可通过后台管理对产品进行购买和续费、短信功能配置等。



管理平台

- 修改资料
- 修改密码
- 短信模块配置
- 重启登陆记录
- 运行程序记录
- 文件修改记录
- 入侵者IP记录
- 发送短信日志
- 注册表修改记录
- 系统用户监控记录
- 退出平台

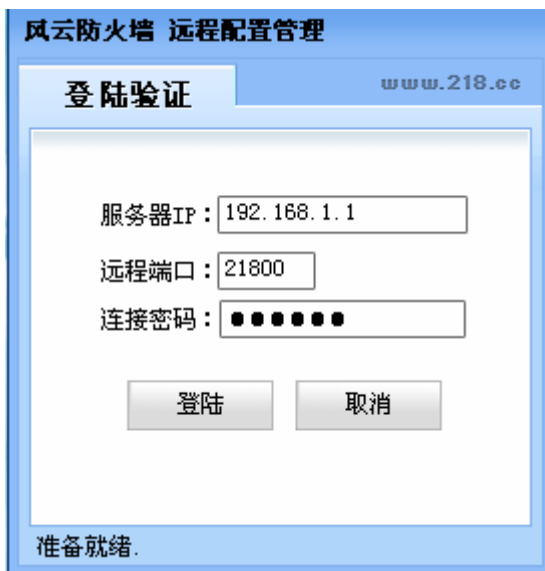
服务器重启登陆记录

61.191.63.197  查询

提交时间	服务器信息	服务器IP
<input type="checkbox"/> 2009-11-06 10:06:31	2009-11-06 10:06:31 用户[Administrator]注销登陆. 端口:3389 IP:61.132.132.219<安徽省合肥市 电信>	61.191.63.197
<input type="checkbox"/> 2009-11-05 16:05:37	2009-11-05 16:05:37 用户[Administrator]登陆系统. 端口:3389 IP:61.191.38.212<安徽省铜陵市 电信>	61.191.63.197
<input type="checkbox"/> 2009-11-04 17:55:08	2009-11-04 17:55:08 用户[Administrator]注销登陆. 端口:3389 IP:121.23.127.130<河北省廊坊市 联通>	61.191.63.197
<input type="checkbox"/> 2009-11-04 17:54:43	2009-11-04 17:54:43 用户[Administrator]解锁登陆. 端口:3389 IP:121.23.127.130<河北省廊坊市 联通>	61.191.63.197
<input type="checkbox"/> 2009-11-04 17:46:05	2009-11-04 17:46:05 用户[Administrator]锁定登陆. 端口:3389 IP:121.23.127.130<河北省廊坊市 联通>	61.191.63.197
<input type="checkbox"/> 2009-11-04 17:31:42	2009-11-04 17:31:42 用户[Administrator]登陆系统. 端口:3389 IP:121.23.127.130<河北省廊坊市 联通>	61.191.63.197

### 3.4 远程设置功能

风云的远程设置功能让您无需登陆服务器也可进行远程配置，只需在本地输入您服务器的 IP 地址，就可以远程操作您的风云，既规避了频繁登陆服务器的风险，又节约了服务器的系统资源。



### 3.5 短信通知功能

短信通知功能是风云防火墙服务器入侵防御系统的一项增值服务（需另外付费，具体费用参阅网站管理后台），



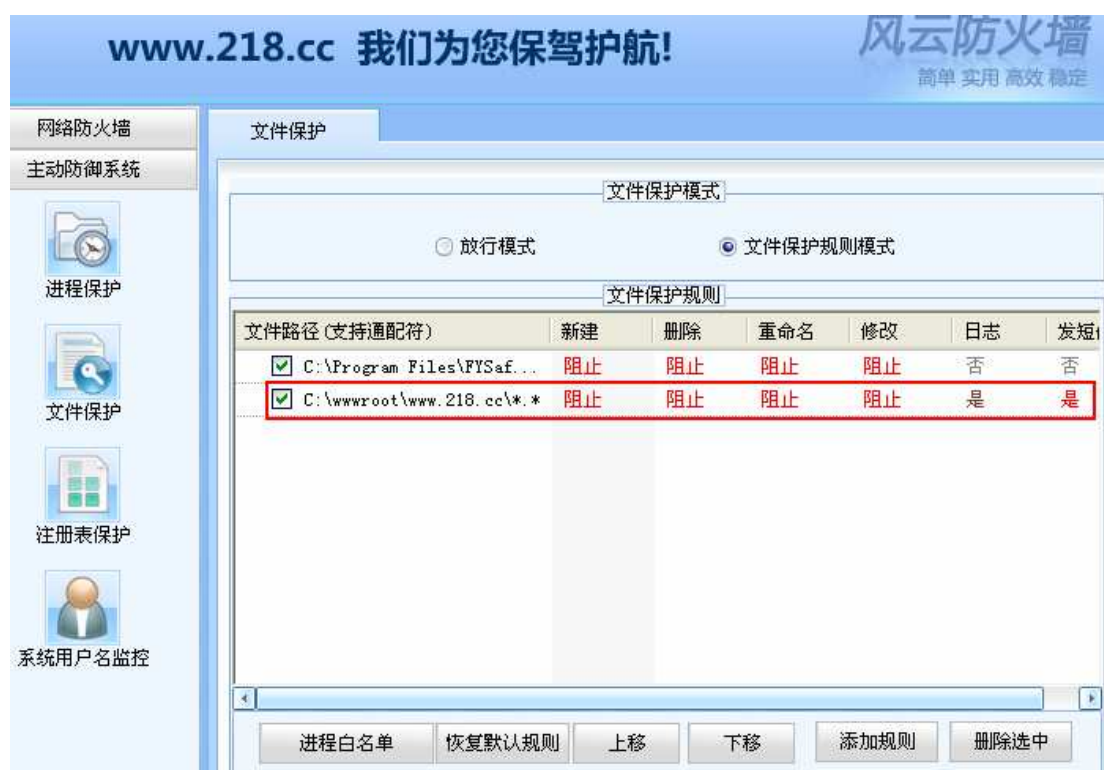
---

它可以为用户及时提供服务器状态通知功能，当用户在设置风云的时候，只需将您需要了解的状态信息选中，风云将会通过后台管理中心的短信平台及时以手机短信息的形式告知用户，让您随时随地轻松掌握服务器运行状态，真正体会信息时代的快捷与精彩。



## FAQ: 1、如何实现主页防篡改功能？

答：主页篡改是由于入侵具有了修改您服务器网站主页文件的权限，为了防止主页被篡改，您可以在“文件保护”设置中将您的网站页面文件设置为“禁止修改、删除”，甚至可以将您整个网站目录设置为不可修改（但请确保您的网站数据库文件可写），再将“文件保护规则”选项选中，如下图：



## 2、为什么我安装了风云后，服务器连接不上？

答：请尝试启用远程配置，查看是否屏蔽了远程连接端口（默认为 3389）、是否禁用了您用来连接服务器的软件，请通过风云远程配置端正确配置后再尝试连接服务器。

## 3、为什么点击“查看日志”后系统没有反应？

答：请查看“进程保护”中是否已禁止风云日志查看器程序



运行，应在进程保护规则中将“风云日志查看器”设置为放行，“风云日志查看器”默认安装在风云防火墙主程序同一目录。



4、我已经设置的保护规则，但是为什么风云并没有按照我设置的规则执行？



答：有时候您设置的保护规则是相互矛盾的，比如您首先设置了禁止在某个文件夹中新建\*.EXE 文件，后又设置了允许在此文件夹内新建任何文件，那么风云将不允许您在此文件夹中新建\*.EXE 文件，因为风云的规则是逐行执行的，当你设置多个规则时，风云是从上往下执行，如上例中，执行了第一条“阻止”规则后就无法再执行下面与之矛盾的“放行”规则了。



## 附录：术语表

**DDOS 攻击:** DDOS 全名是 Distribution Denial of service (分布式拒绝服务攻击), 很多 DDOS 攻击源一起攻击某台服务器就组成了 DDOS 攻击, DDOS 最早可追述到 1996 年最初, 在中国 2002 年开始频繁出现, 2003 年已经初具规模. DDOS 的攻击方式有很多种, 最基本的 DDOS 攻击就是利用合理的服务请求来占用过多的服务资源, 从而使服务器无法处理合法用户的指令。

**SQL 注入:** 所谓 SQL 注入, 就是通过把 SQL 命令插入到 Web 表单递交或输入域名或页面请求的查询字符串, 最终达到欺骗服务器执行恶意的 SQL 命令, 比如先前的很多影视网站泄露 VIP 会员密码大多就是通过 WEB 表单递交查询字符暴出的, 这类表单特别容易受到 SQL 注入式攻击。

当应用程序使用输入内容来构造动态 sql 语句以访问数据库时, 会发生 sql 注入攻击。如果代码使用存储过程, 而这些存储过程作为包含未筛选的用户输入的字符串来传递, 也会发生 sql 注入。sql 注入可能导致攻击者使用应用程序登陆在数据库中执行命令。如果应用程序使用特权过高的帐户连接到数据库, 这种问题会变得很严重。在某些表单中, 用户输入的内容直接用来构造 (或者影响) 动态 sql 命令, 或者作为存储过程的输入参数, 这些表单特别容易受到 sql 注入的攻击。而许多网站程序在编写时, 没有对用户输入的



---

合法性进行判断或者程序中本身的变量处理不当，使应用程序存在安全隐患。这样，用户就可以提交一段数据库查询的代码，根据程序返回的结果，获得一些敏感的信息或者控制整个服务器，于是 sql 注入就发生了。