等级：**F**

服务器安全狗 Linux 版 V2.5
用户手册

厦门服云信息科技有限公司

www.safedog.cn

2015 年 04 月

目录

1. 软件说明

服务器安全狗 Linux 版（SafeDog for Linux Server）是为 Linux 服务器开发的一款服务器管理软件，它集成了 DDOS 攻击检测和防御系统、远程登录监控、ssh 防暴力破解、流量统计、帐户监控和设置、系统参数快速设置、系统运行状态展示、系统状态实时监控等功能。其 DDOS 攻击检测和防御系统能够有效防御 cc 攻击，并极大地减少误判。本软件提供纯字符界面下的界面交互接口和详细的操作指引，使得管理员对服务器的状态更加了解，管理和配置服务器也更加简单。

2. 软件运行环境

软件当前版本支持的 linux 服务器的操作系统包括：Ubuntu 、Centos 、Fedora 和 RHEL 等发行版的较新版本，如果安装过程中提示无法安装表示系统版本太老等原因安全狗目前不支持。请根据您的系统选择 32 位安装包或 64 位安装包。

3. 软件安装

以 32 位安装包为例，64 位安装包把对应的 32 改成 64 即可。

步骤 1：到 http://safedog.cn 下载软件发布包(.tar.gz 格式)：`safedog_linux32.tar.gz`

也可以采取 `wget` 的方式下载发布包：

```
wget http://safedog.cn/safedog_linux32.tar.gz
```

步骤 2：在 root 帐户下执行以下命令：

```
tar xzvf safedog_linux32.tar.gz
cd safedog_linux32
chmod +x *.py
./install.py
```

步骤 3：完成安装后可运行命令 **`sdui`** 进入操作界面，如图 3.1。

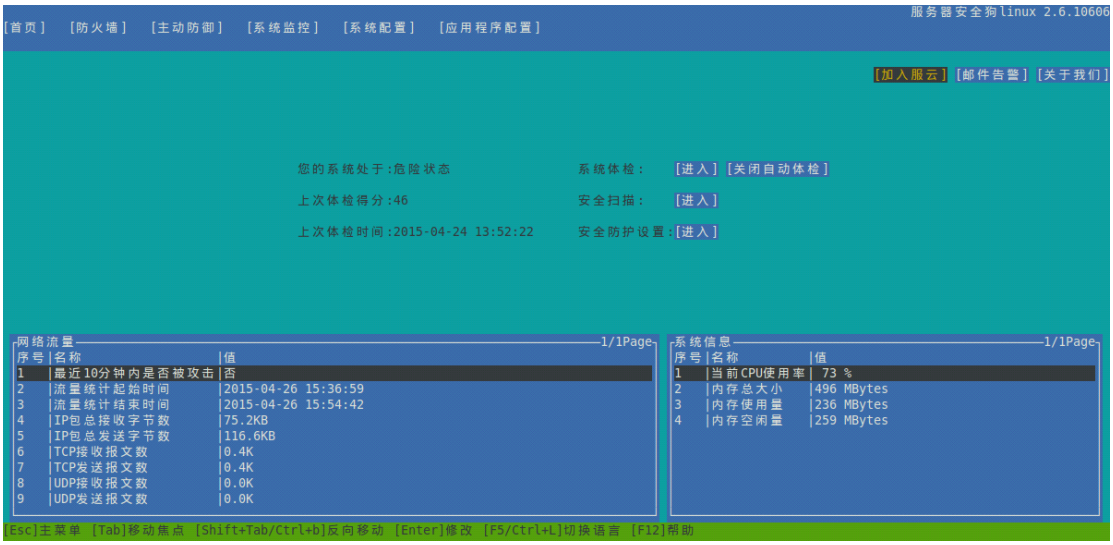


图 3.1 服务器安全狗 Linux 版-主界面

4. 软件运行

直接运行命令：**sdui**

即可进入软件操作界面，如图 3.1，进入软件后，请详细阅读每个界面最底部的操作提示，按操作提示进行操作。

使用：

service safedog status 查看安全狗服务；

service safedog start 启动安全狗服务；

service safedog stop 停止安全狗服务；

sdstart 重启安全狗服务。

首次进入 sdui 界面的首页，连续按 F5 或 CTRL+L 组合键，切换到合适的显示文字。

在软件的每个界面直接按 F12，可以显示详细的帮助信息。

5. 软件功能说明

重要提醒：

✧ 软件的防火墙等功能依赖于 iptables，在使用软件时，请勿随意修改 iptables，否则可能造成软件功能异常。建议修改 iptables 之后，执行 sdstart 重启安全软件服务。

5.1 首页

5.1.1 系统体检

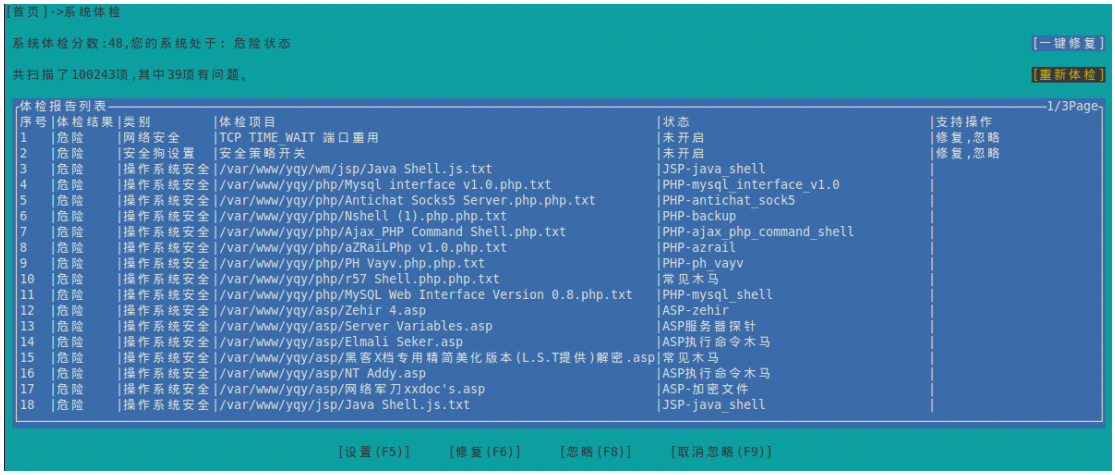


图 5.1.1 首页-系统体检

系统体检功能通过对系统进行全方位体检，检测各种可能出现的安全漏洞，并提供相应的修复功能，有效的帮助用户提高服务器安全性与稳定性。如发现问题，用户可根据提示立即修复系统，以提高服务器性能。同时，若服务器已经加入服云，则体检结果将上传至云端，从云端可以直观地看到体检结果，

支持进行自动体检，开启时，则系统会在凌晨进行自动体检。

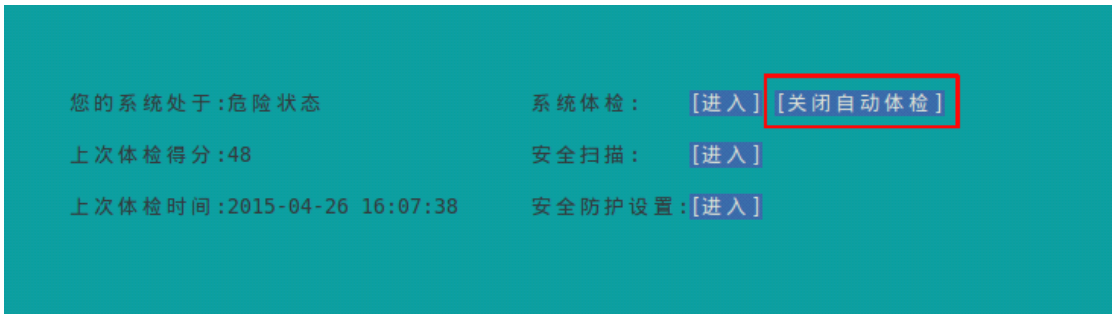


图 5.1.2 首页

5.1.2 安全扫描

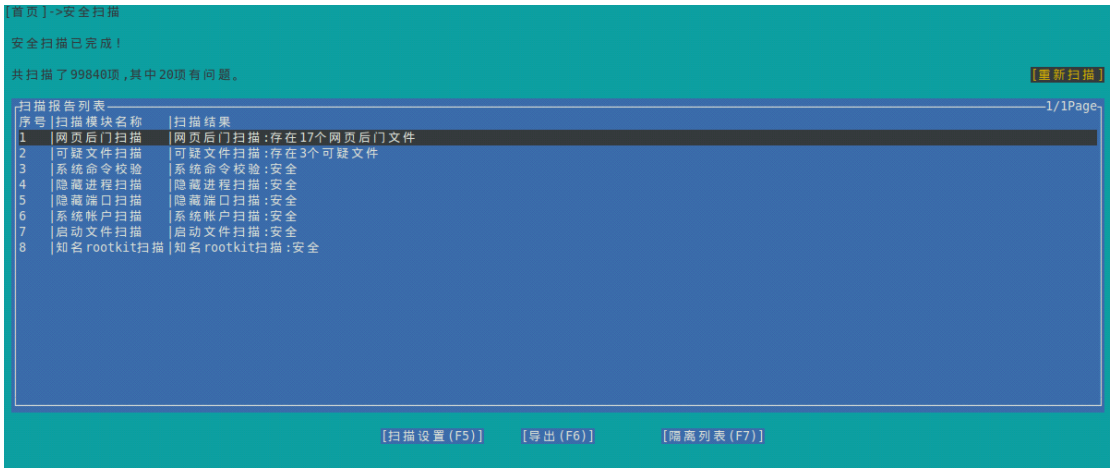


图 5.1.3 首页-安全扫描

安全扫描从系统安全层面，对用户常关心的 8 个方面，进行扫描，可以根据扫描结果，采取相应措施，提高系统安全性。

（1）开始扫描：针对用户设置的扫描模块，进行扫描。

（2）扫描报告列表：显示扫描后的结果，如图 5.1.3。选中某一行，点击回车，即可显示具体的危险项目，以网页后门扫描模块为例，如图 5.1.4。支持加入白名单或者隔离操作，同时可以到相应的白名单列表或者隔离列表查看列表具体内容。

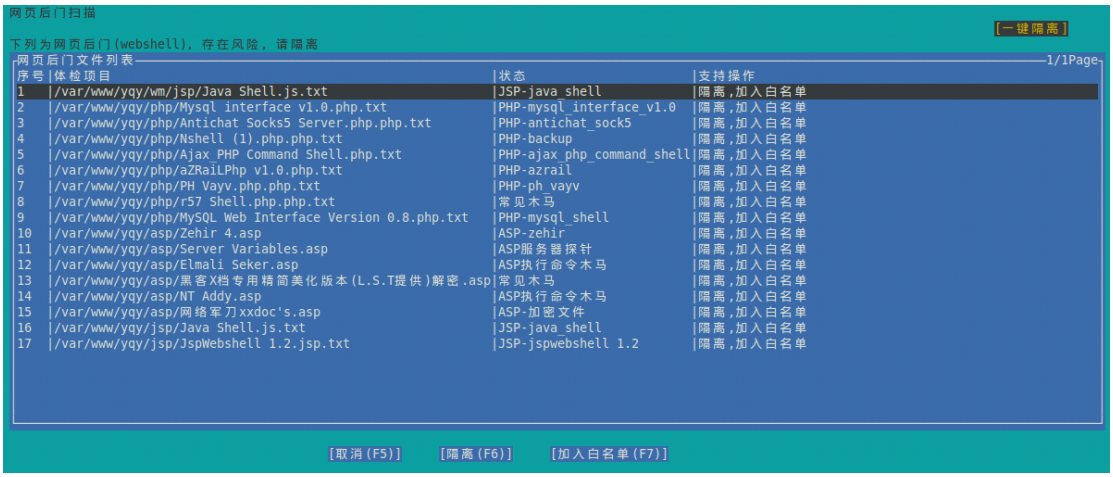


图 5.1.4 安全扫描-网页后门扫描

（3）扫描设置：设置需要参与扫描的模块。如图 5.1.5。

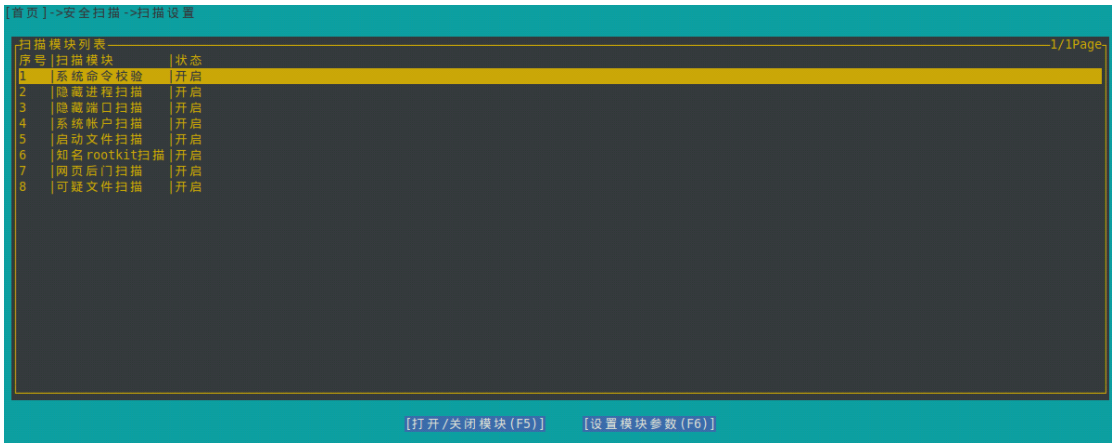


图 5.1.5 安全扫描-扫描设置

包括 8 大扫描模块：系统命令校验、隐藏进程扫描、隐藏端口扫描、系统账户扫描、启动文件扫描、知名 rootkit 扫描、网页后门扫描、可疑文件扫描。

❖ 打开/关闭模块：开启或者关闭列表中选中模块。开启时，则参与安全扫描，否则，不参与扫描。

❖ 设置模块参数：详细设置列表中选中模块，比如设置扫描路径、扫描类型等。每个模块，都支持设置白名单列表，列表中的命令、进程等，被认为是安全的，不参与扫描。

❖ 系统命令校验：支持自定义扫描命令列表。自定义扫描命令是指用户自己安装的非系统自带的可信软件。

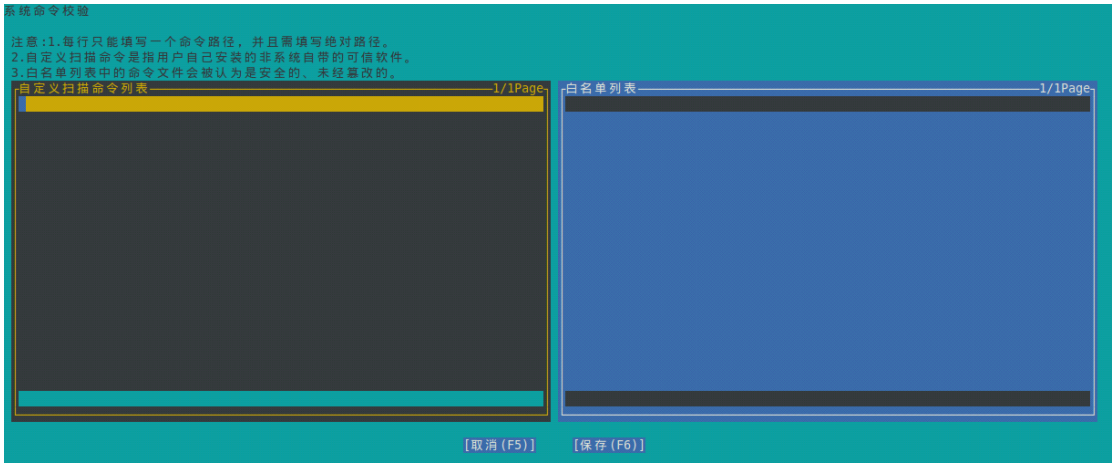


图 5.1.6 安全扫描-系统命令校验

❖ 启动文件扫描：支持设置启动文件列表。启动列表中的所有文件和目录都将参与扫描，并且若填写的是目录路径，则其子目录及目录下的文件均参与扫描。

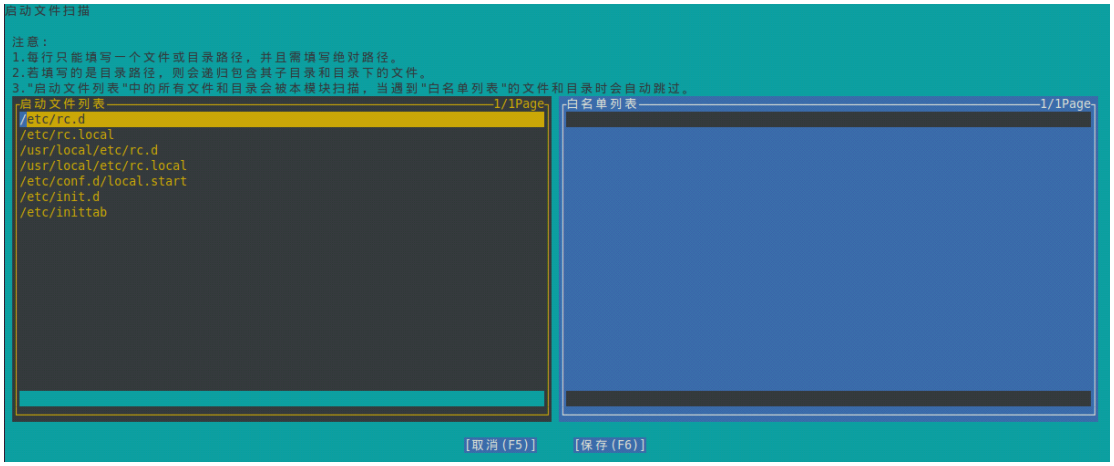


图 5.1.7 安全扫描-启动文件扫描

❖ 网页后门扫描：

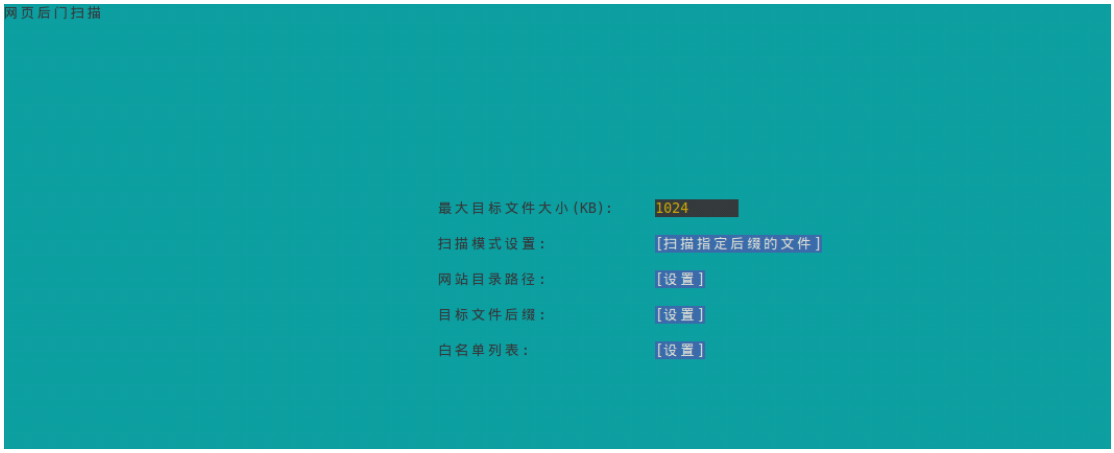


图 5.1.8 安全扫描-网页后门扫描

■ 最大目标文件大小：大于此设置值的文件，不参与扫描。

■ 扫描模式设置：支持两种模式，扫描指定后缀文件、扫描所有类型的文件。

当扫描模式为扫描指定后缀文件时，将扫描所设置的目标文件后缀，非此列表中的文件不参与扫描。

当扫描模式为扫描所有类型文件时，将扫描所有文件，与目标文件后缀无关。

■ 网站目录路径：设置网站目录的路径。

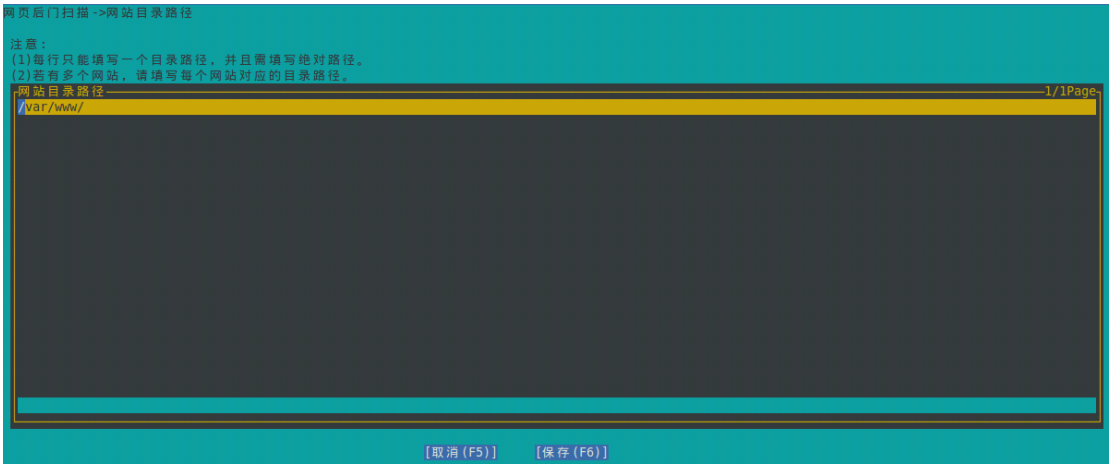


图 5.1.9 网页木马扫描-网站目录路径

- 目标文件后缀：软件默认携带部分目标文件后缀，同时支持用户自定义。

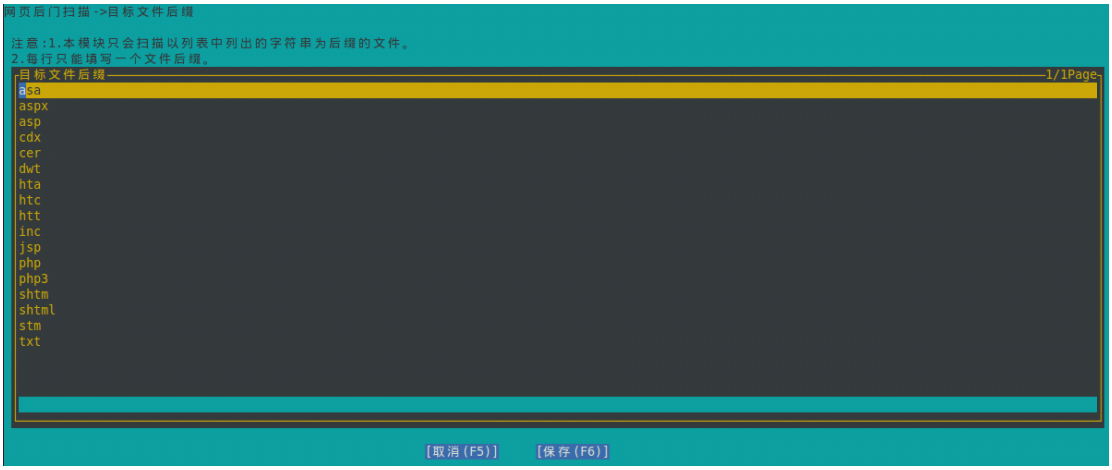


图 5.1.10 网页后门扫描-目标文件后缀

- 可疑文件扫描：

图 5.1.11 安全扫描-可疑文件扫描

扫描模式设置：支持两种模式设置，快速扫描、全盘扫描。

（4）导出：导出扫描的结果列表。如图 5.1.12。

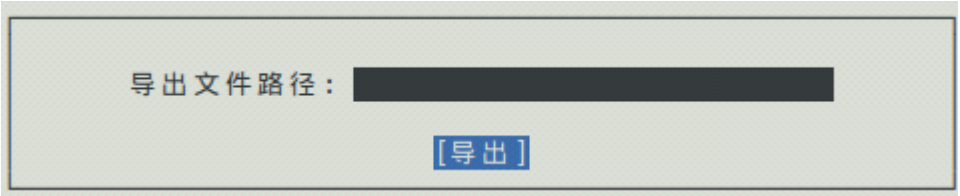


图 5.1.12 安全扫描-导出

（5）隔离列表：查看所有隔离文件，如图 5.1.13。隔离列表中的项目支持恢复和删除，删除操作不可逆，请谨慎。

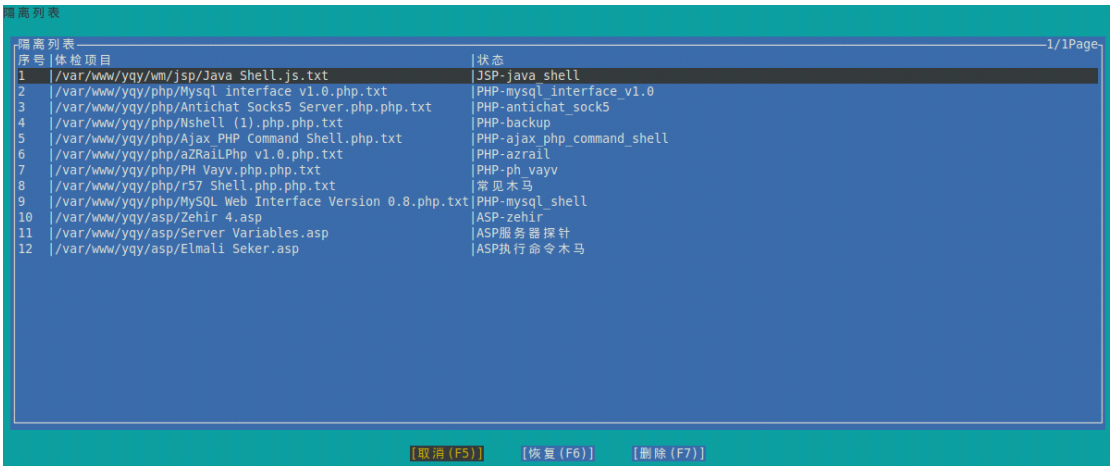


图 5.1.13 安全扫描-隔离列表

5.1.3 加入服云

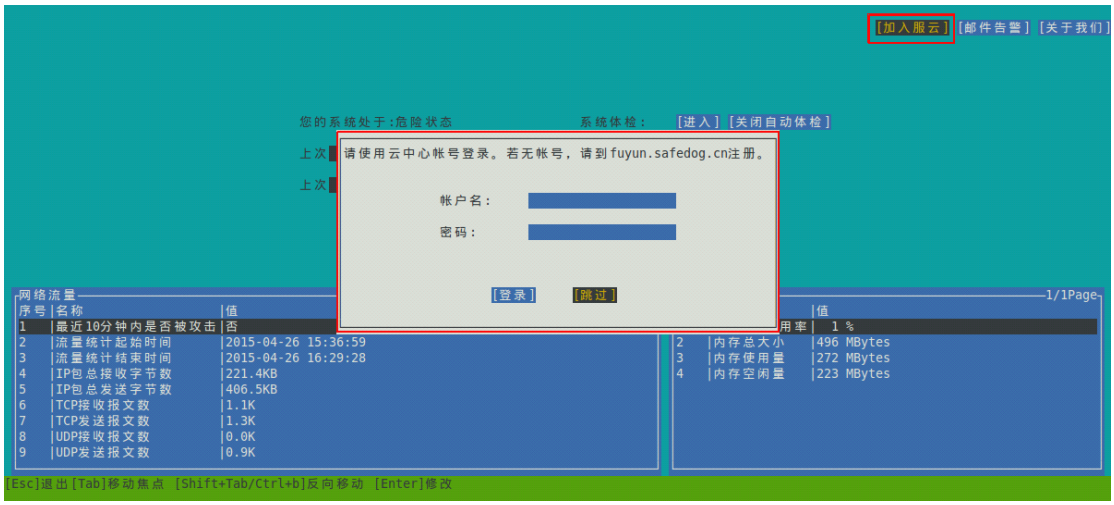


图 5.1.14 首页-加入服云

通过输入服云帐号的用户名和密码，自动下载证书，加入服云。

❖ 此功能必须保证已经拥有服云帐号，若没有帐号，请先到官网注册。

- 支持输入以下命令加入服云：**sdcloud -u 用户名**

```
root@yqy-virtual-machine:/home/yqy# sdcloud -u 服云
Enter password:
Error[-3]:Failed to login. Incorrect user name or password.
```

图 5.1.15 加入服云（命令行方式）

- 软件界面不支持中文用户名和中文密码，此类情况通过以上命令加入。
- 软件可以通过下面的命令查看加入服云的命令使用方法：**sdcloud -h**

```
root@yqy-virtual-machine:/home/yqy# sdcloud -h
Usage:sdcloud -u your_user_name
-h,--help                   Display this usage information.
-v,--version                Display the version of this program.
-u,--user                   set the account name of server cloud .
```

图 5.1.16 查询加入服云的命令方式

5.2 防火墙

5.2.1 网络防火墙

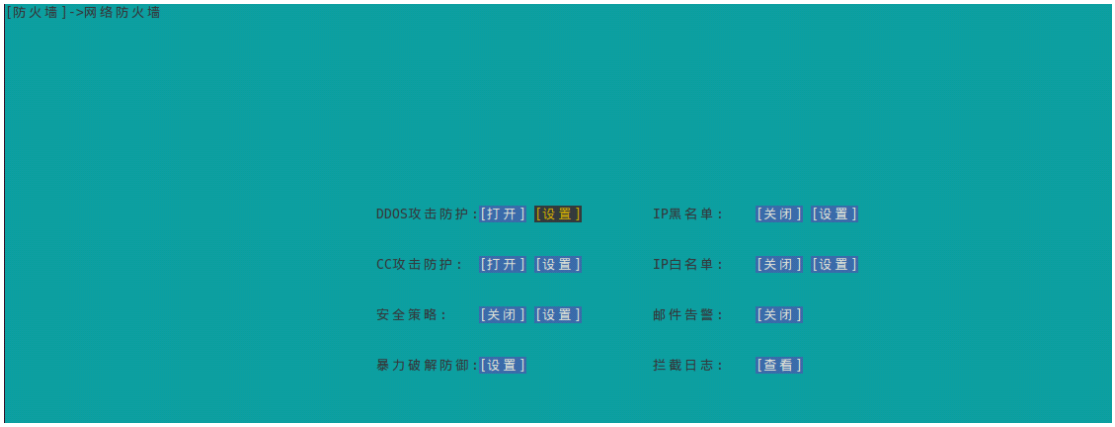


图 5.2.1 网络防火墙

（1）DDOS 攻击防护

- 打开/关闭：设置 DDOS 攻击防护功能的开关。
- 设置：设置 DDOS 攻击防护规则，详见 5.2.1.1 章节。

（2）CC 攻击防护

- 打开/关闭：设置 CC 攻击防护功能的开关。
- 设置：设置 CC 攻击防护规则，详见 5.2.1.2 章节。

（2）安全策略

- 打开/关闭：设置安全策略防护功能的开关。
- 设置：设置安全策略防护规则，详见 5.2.1.3 章节。

（3）暴力破解防御：支持 FTP 和 SSH 防暴力破解，详见 5.2.1.4 章节。

（4）IP 黑名单

- 打开/关闭：设置 IP 黑名单功能的开关。
- 设置：设置 IP 黑名单，详见 5.2.1.5 章节。

（5）IP 白名单

- 打开/关闭：设置 IP 白名单功能的开关。
- 设置：设置 IP 白名单，详见 5.2.1.6 章节。

注意：IP 黑名单的优先级高于 IP 白名单。

（6）邮件告警：开启后，若拦截网络攻击，则通过邮件告警方式提醒用户。此功能必须基于邮件告警相关信息已经成功设置，详见 5.5.4 章节。

（7）拦截日志：软件界面上仅显示最近的拦截信息，并且在关闭拦截后清空。

拦截的报告文件： **/etc/safedog/monitor/antiddos.txt**

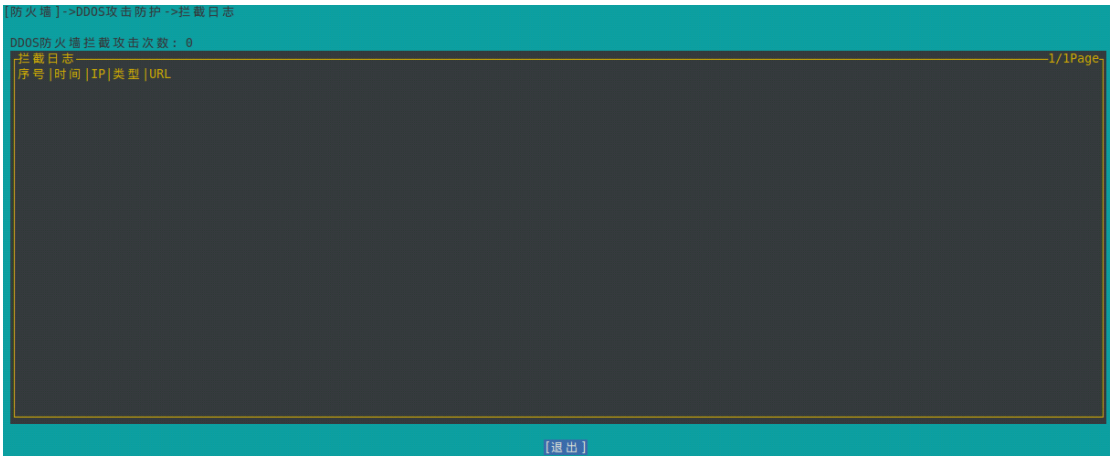


图 5.2.2 网络防火墙-拦截日志

- 拦截过程中，可以通过下面的命令查看当前已拦截的 IP 数：

```
iptables -nL ANTI_DDOS | wc -L
```

可以通过下面的命令查看拦截 IP 的过程：

```
tail -f /etc/safedog/monitor/antiddos.txt
```

5.2.1.1 DDOS 攻击防护

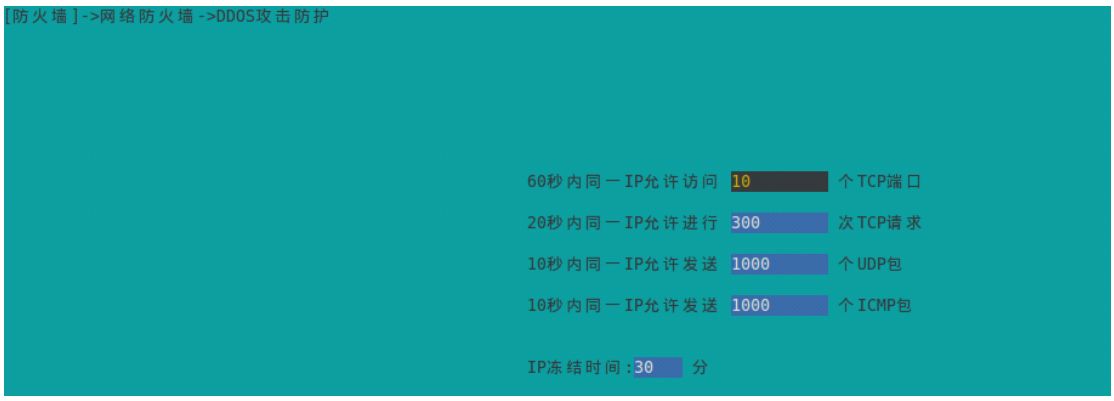


图 5.2.3 网络防火墙-DDOS 攻击防护

本功能依赖于 iptables，如果 iptables 不能正常工作，则本功能无效。

（1）冻结攻击 IP 的时长：10~1000

（2）同一 IP 在 60 秒内访问超过 N 个 TCP 端口进行拦截：同一个 IP 在 1 分钟内访问超过设置的 TCP 端口数目，则进行拦截。

（3）同一 IP 在 20 秒内进行 TCP 请求超过 N 次进行拦截：同一个 IP 在 20 秒内 TCP 请求超过设置的次数上限时，则进行拦截。

（4）同一 IP 在 10 秒内发送过来 UDP 包超过 N 个进行拦截：同一个 IP 在 10 秒内发送 UDP 包的数目超过设置上限时，则进行拦截。

（5）同一 IP 在 10 秒内发送过来 ICMP 包超过 N 个进行拦截：同一个 IP 在 10 秒内发送 ICMP 包的数目超过设置上限时，则进行拦截。

5.2.1.2 CC 攻击防护

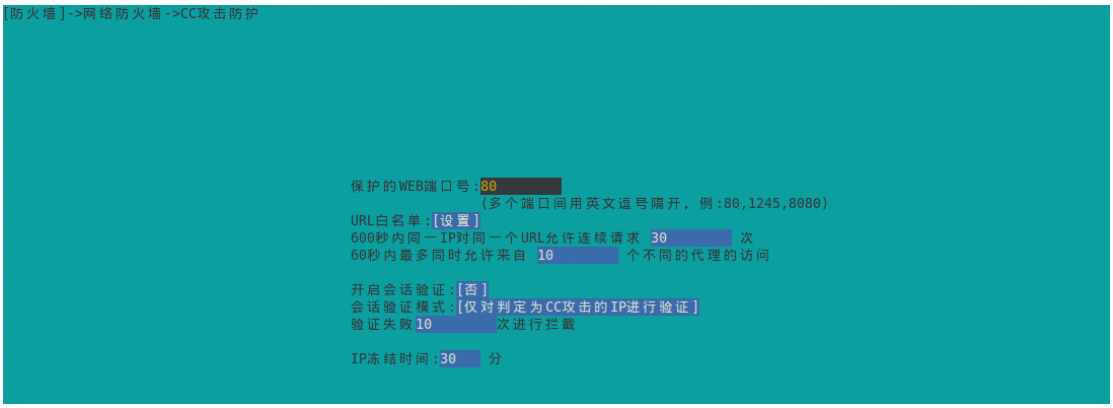


图 5.2.4 网络防火墙-CC 攻击防护

（1）WEB 端口号：提供 web 服务的端口，默认为 80，可以修改，多个端口之间用英文逗号隔开。

（2）URL 白名单：以名单中的项作开头的 URL 进行的访问不会被当成攻击。如添加

"/image/"到白名单中，则对"/image/a.jpg"的访问不会被当成攻击。

（3）60 秒内同一 IP 连续对同一个 URL 请求超过 N 次进行拦截：5~30。

（4）60 秒内最多同时允许来自 N 个不同的代理的访问：0~9999。

（5）启用会话验证：对所有访问或疑似攻击的访问进行会话验证，如果是正常用户访问网站误判为攻击的，启用会话验证时可以避免这种误判拦截。

（6）选择会话验证模式：正常情况下使用“仅对判定为 CC 攻击的 IP 进行验证”；当正在被攻击时，可以切换为“对所有访问 IP 都进行验证”。

（7）验证失败 N 次进行拦截：5~30。

（8）冻结攻击 IP 的时长：10~1000。

5.2.1.3 安全策略

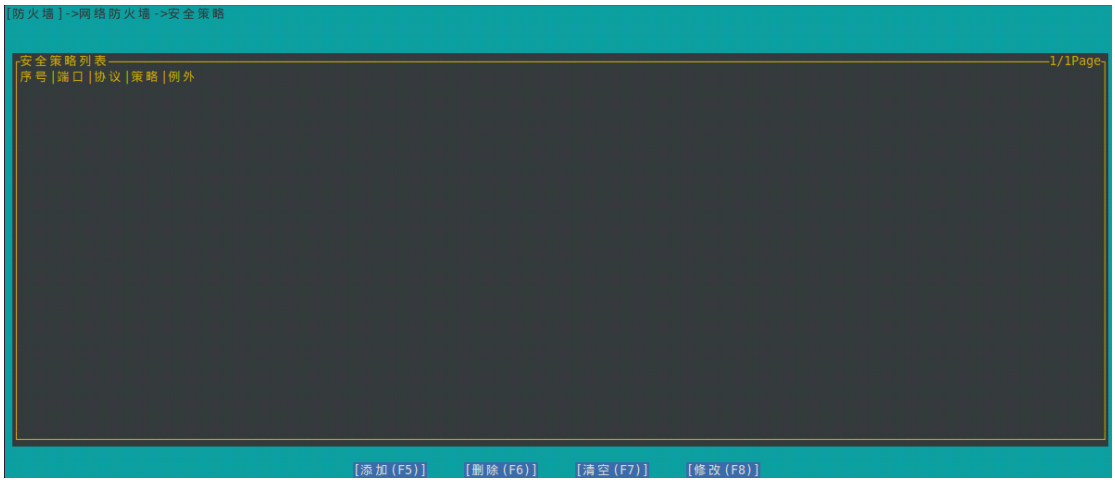


图 5.2.5 网络防火墙-安全策略

可以针对网络端口自定义安全策略，对指定的端口允许或阻止所有 IP 访问，可设置例外 IP，例外 IP 不受该条安全策略的影响（既不会被拦截，也不会被信任）。

（1）添加：添加安全策略规则。如图 5.2.6。

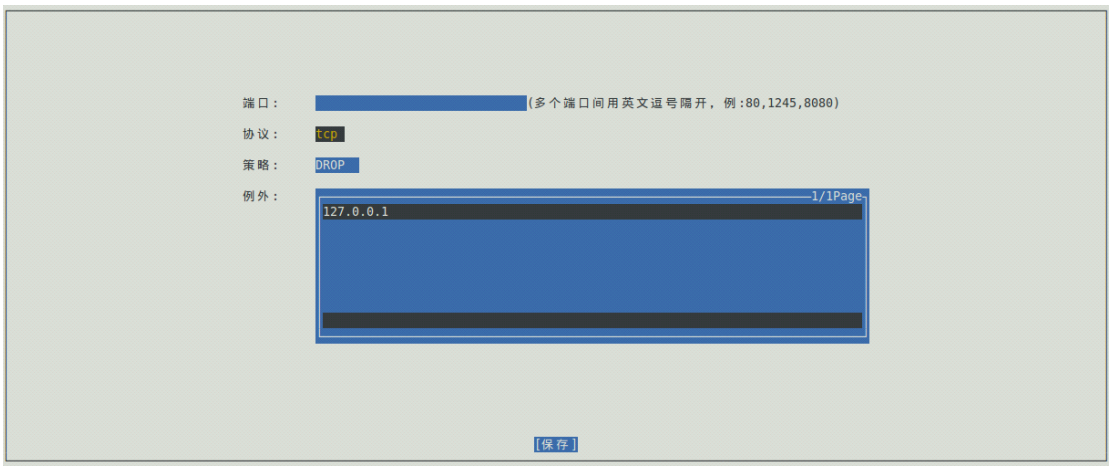


图 5.2.6 安全策略-添加

- 端口：设置受规则约束的端口，支持多个端口同时设置。
- 协议：支持四种协议，即 TCP、UDP、ICMP、IGMP。
- 策略：支持两种策略，即 ACCEPT 和 DROP。
- 例外：若选择 ACCEPT 策略，则此列表中所有 IP 一律拒绝；反之，一律接受。

（2）删除：删除所选规则。

（3）清空：删除列表中所有规则。

（4）修改：修改所选规则。如图 5.2.6。

注意：

- 每个协议的每个端口只允许添加一条策略，否则在添加时会提示冲突。

5.2.1.4 暴力破解防御

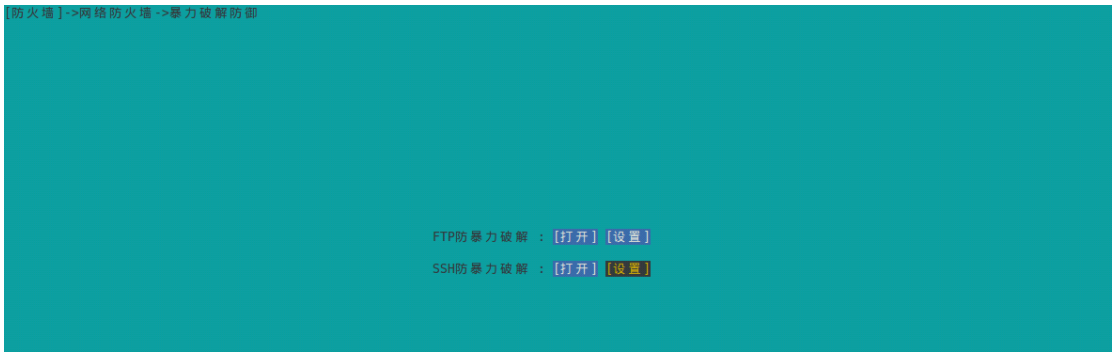


图 5.2.7 网络防火墙-暴力破解防御

（1）FTP 防暴力破解

- 打开：打开或关闭 FTP 登录破解防护的功能开关。
- 设置：

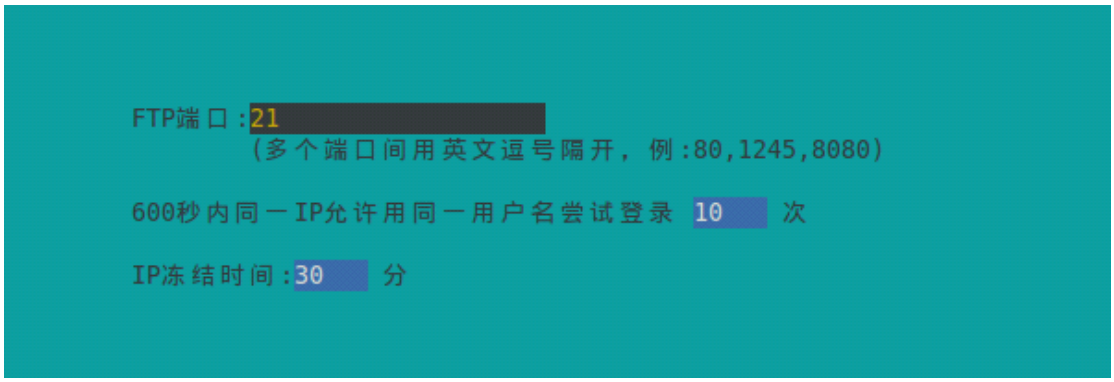


图 5.2.8 FTP 防暴力破解-设置

- FTP 端口：设置 FTP 保护端口，支持设置多端口。
- 600 秒内同一 IP 允许用同一用户名尝试登录 N 次：启用 FTP 登录破解防护功能时，当受保护端口，同一 IP 在 600 秒内用同一用户名登录，密码错误超过设置值时，将进行拦截。
- IP 冻结时间：10~1000。

（2）SSH 防暴力破解

- 打开：打开或关闭 SSH 登录破解防护的功能开关。
- 设置：

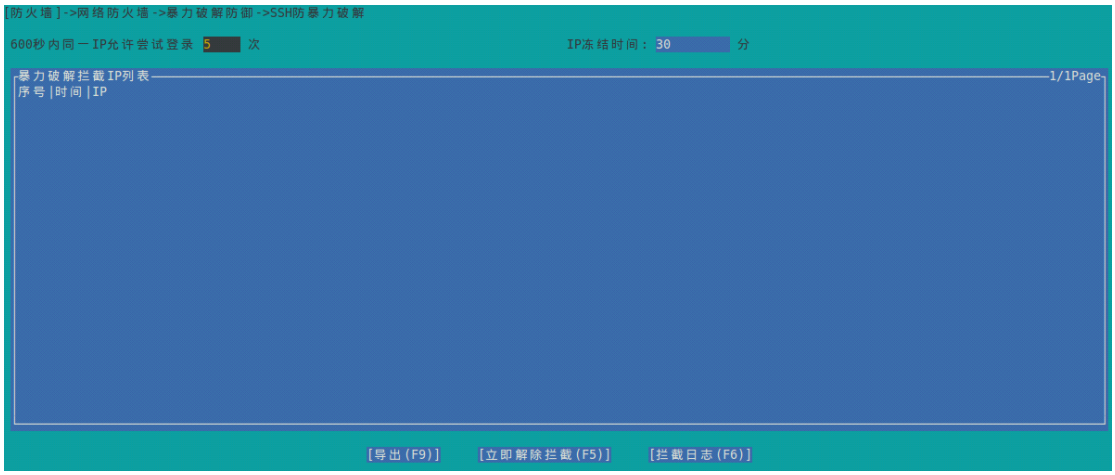


图 5.2.9 SSH 防暴力破解-设置

- 600 秒内同一 IP 登录允许尝试登录 N 次：某 IP 在远程客户端用密码登录时最多能重试的次数，如果错误次数超过该值，该 IP 就会被拦截一段时间。
- IP 冻结时间：拦截可疑 IP 的时间长度，允许范围 10~1000。当超过该时间时，会自动解除对该 IP 的拦截。
- 暴力破解拦截 IP 列表：显示当前被拦截登录的所有 IP。当某 IP 的拦截被解除时，该 IP 会从该列表中删除。

■ 导出：将暴力破解拦截 IP 列表导出到指定文件。如图 5.2.10。

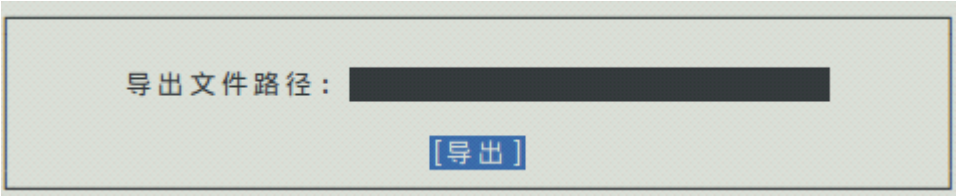


图 5.2.10 SSH 防暴力破解-导出

■ 立即解除拦截：对拦截 IP 列表中选中的帐户，立即解除。解除后，该 IP 可以立即重新登录。

■ 拦截日志：查看因暴力破解而被拦截的所有历史记录。

图 5.2.11 SSH 防暴力破解-拦截日志

5.2.1.5 IP 黑名单

IP 黑名单表示名单中的 IP 在 DDOS 防护启动后直接拦截掉。

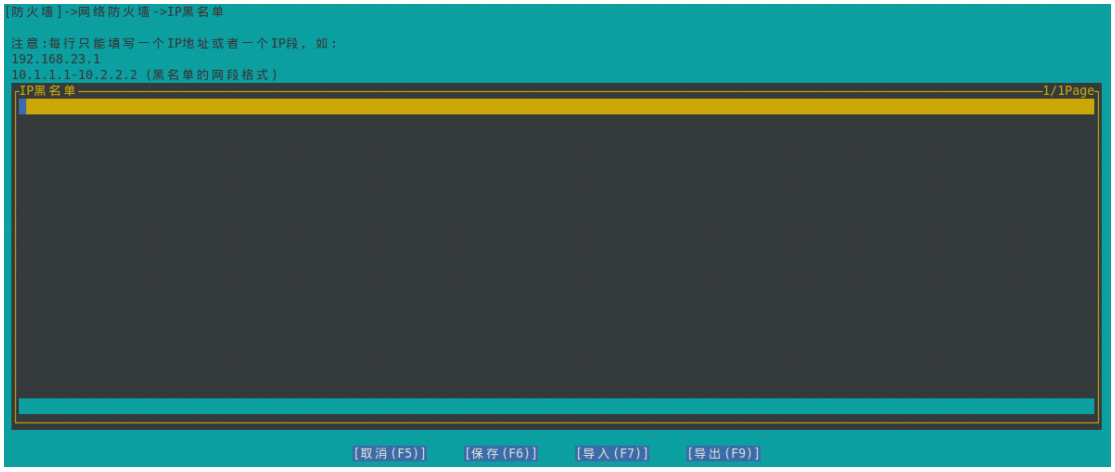


图 5.2.12 网络防火墙-IP 黑白名单

5.2.1.6 IP 白名单

IP 白名单表示名单中的 IP 或 IP 段不会被当成攻击 IP。

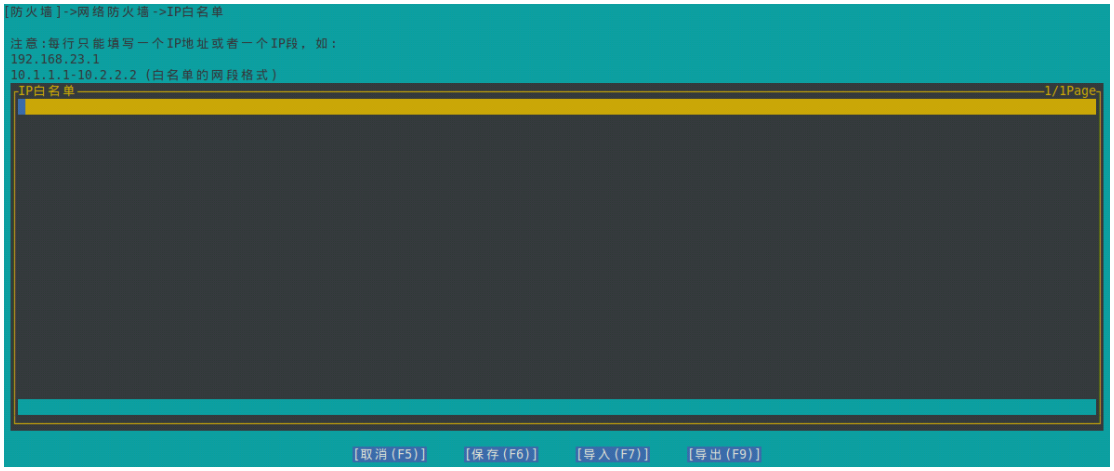


图 5.2.13 DDOS 攻击防护-IP 白名单

5.2.2 TCP 连接状态

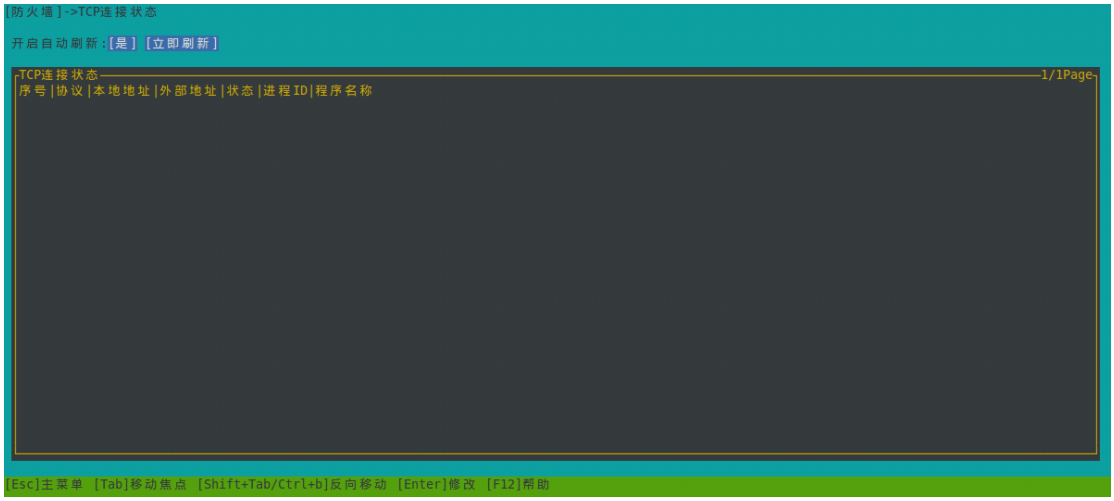


图 5.2.14 防火墙-TCP 连接状态

显示当前系统中 TCP 连接的状态及相应的地址、进程 ID 和进程名字。

（1）开启/关闭自动刷新：开启时，每隔几秒将自动获取当前系统 TCP 连接状态。

（2）立即刷新：立即获取当前系统中 TCP 连接状态。

注意：

❖ 在受到攻击时避免进入该菜单，因为被攻击时，系统中的连接数非常多，可能响应延迟较高。

5.2.3 TCP 监听端口

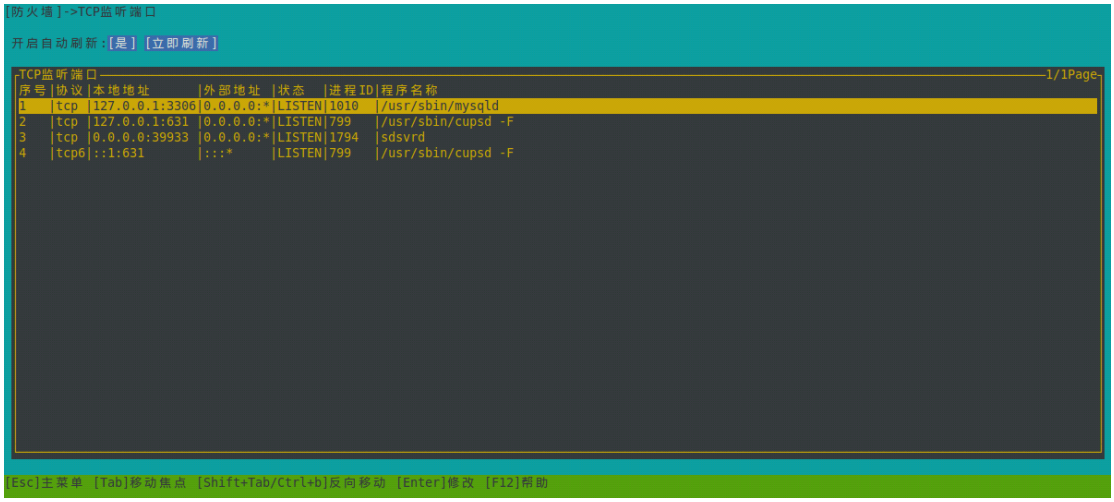


图 5.2.15 防火墙-TCP 监听端口

显示当前系统中正在监听的 tcp 端口及相应的地址、进程 ID 和进程名字。

（1）开启/关闭自动刷新：开启自动刷新时，每隔几秒将自动获取当前系统正在监听的 TCP 端口状态。

（2）立即刷新：立即获取当前系统系统正在监听的 TCP 端口状态。

5.3 主动防御

5.3.1 系统帐户保护

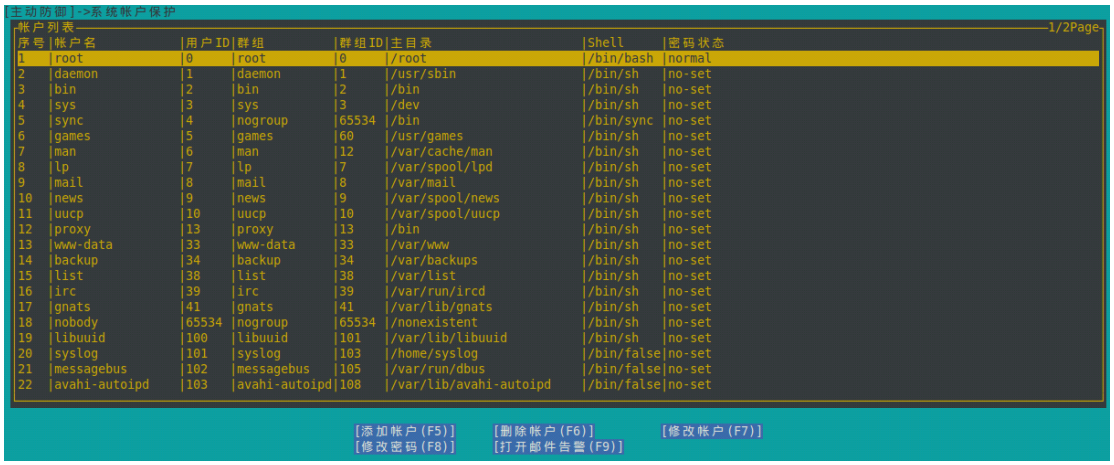


图 5.3.1 主动防御-系统帐户保护

显示当前系统中所有帐户的详细信息。

（1）添加帐户：添加系统帐户，如图 5.3.2，其中帐户名为必填项，其余为可选项。

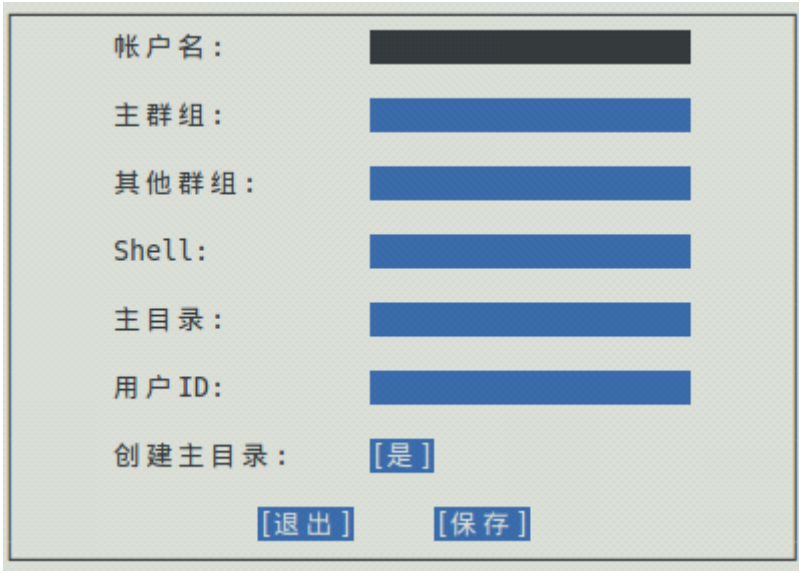


图 5.3.2 系统帐户保护-添加

（2）删除帐户：删除选中的系统帐户。

（3）修改帐户：修改选中的系统帐户，如图 5.3.3。

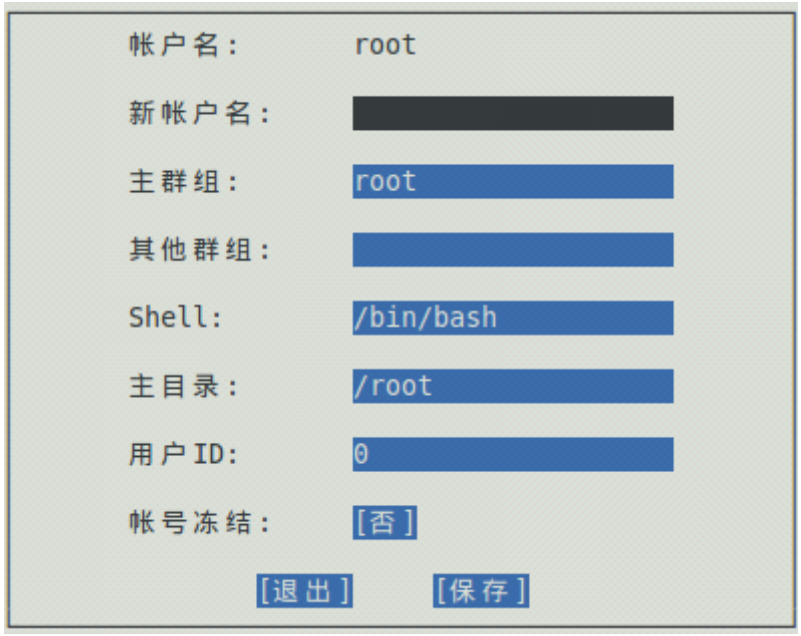


图 5.3.3 系统帐户保护-修改

（4）修改密码：修改选中的系统帐户的密码，如图 5.3.4。

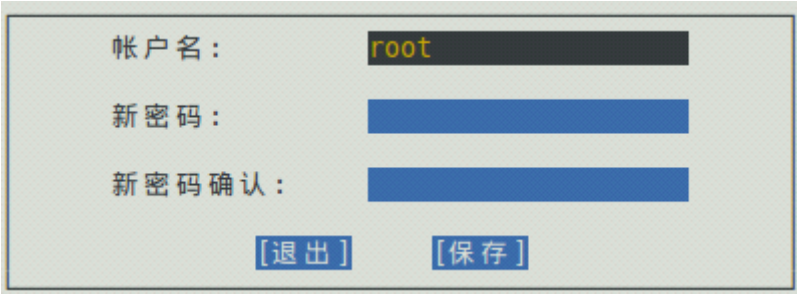


图 5.3.4 系统帐户保护-修改密码

（5）打开邮件告警：系统帐户保护的信息，通过邮件告警方式提醒用户。此功能必须基于邮件告警相关信息已经成功设置，详见 5.5.5 章节。

注意：

- 如果您不是十分清楚自己在做什么，请不要对 root 用户和 root 组做任何操作。
- 日志文件： **/etc/safedog/monit/accountmonit.txt**

5.3.2 SSH 远程登录保护

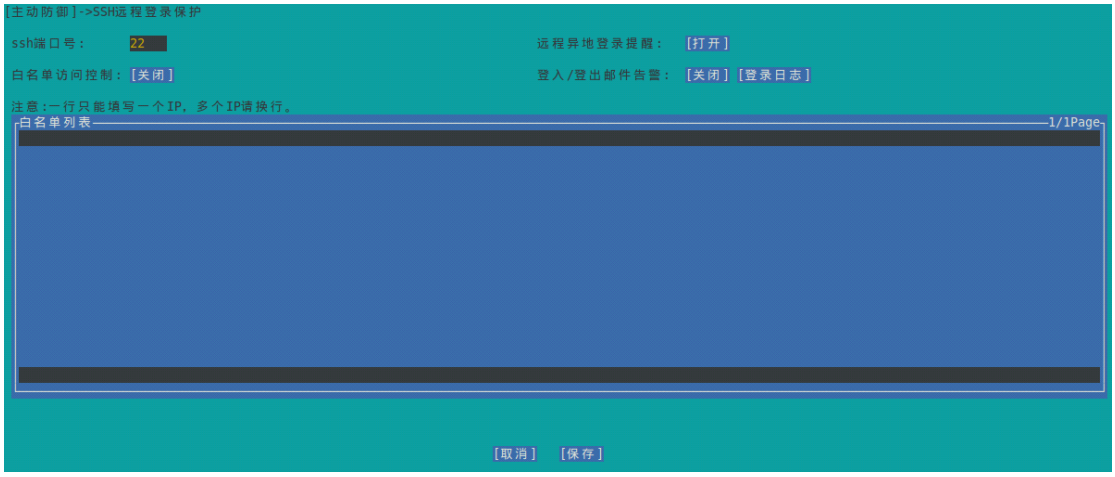


图 5.3.5 主动防御-远程登录保护

主要用来防止黑客通过 ssh 进行非法的远程登录，并可查看登录日志，支持设置 IP 白名单。

（1）ssh 端口号：设置 ssh 端口号。

（2）远程异地登录提醒：实时获取当前系统的远程登录情况，同时结合云端设置常用地和手机或者邮箱，当发现非常用地登录时，将进行通知告警，有效防止非法入侵。

（3）白名单访问控制：若选择“开启”，则系统只允许白名单列表中的 IP 进行 ssh 登录。

（4）登入/登出邮件告警：通过邮件发送系统登录日志。此功能必须基于邮件告警相关信息已经成功设置，详见 5.5.5 章节。

登录日志：查看成功登录到系统的所有历史记录。

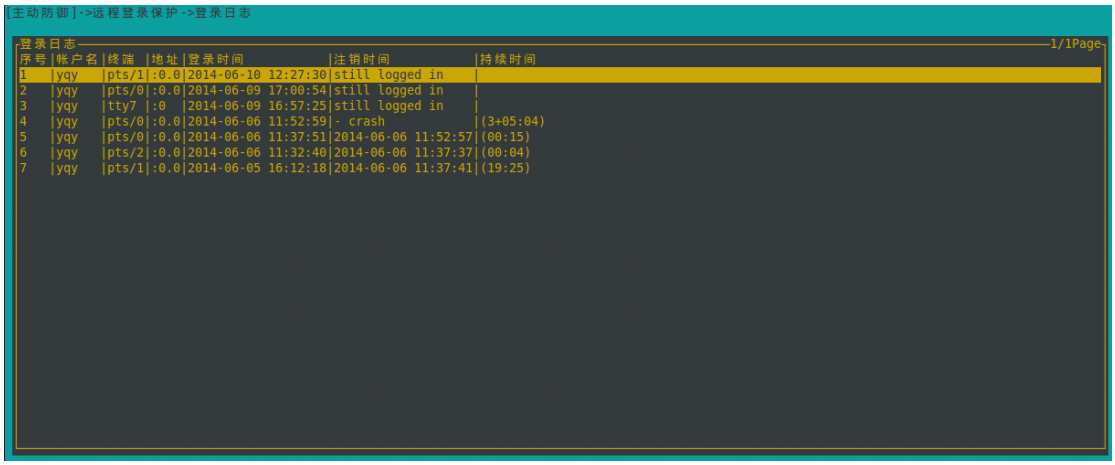


图 5.3.6 远程登录保护-登录日志

注意：

❖ 确保已经将本地机器的外部 IP 添加到白名单列表中，否则设置过后就把自己关在服务器门外，连不上服务器，只能通过以下办法重新恢复连接：要求机房管理员重启电脑，重启后白名单机制会禁用。

❖ 日志文件：**/etc/safedog/monit/loginmonit.txt**

5.4 系统监控

5.4.1 文件监控

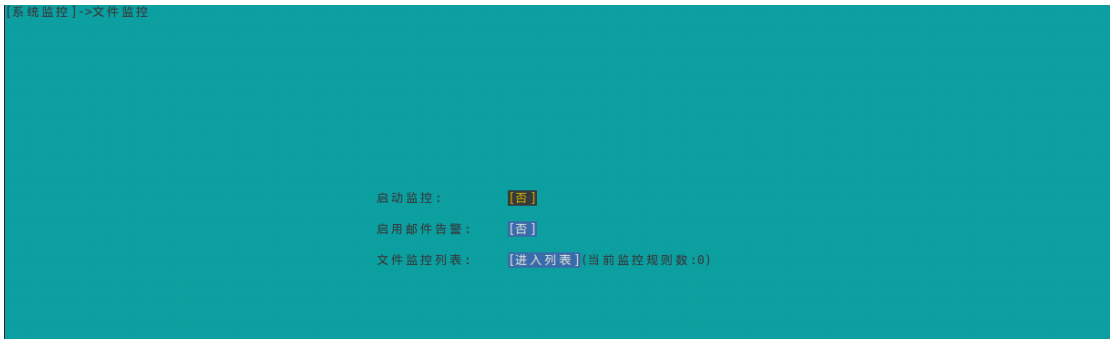


图 5.4.1 系统监控-文件监控

（1）启动监控：文件监控的功能开关。

（2）启用邮件告警：通过邮件发送监控记录给用户。此功能必须基于邮件告警相关信

息已经成功设置，详见 5.5.5 章节。

（3）文件监控列表：列表列出所要监控的所有文件和目录，设置完文件列表后，再开启监视器开关。

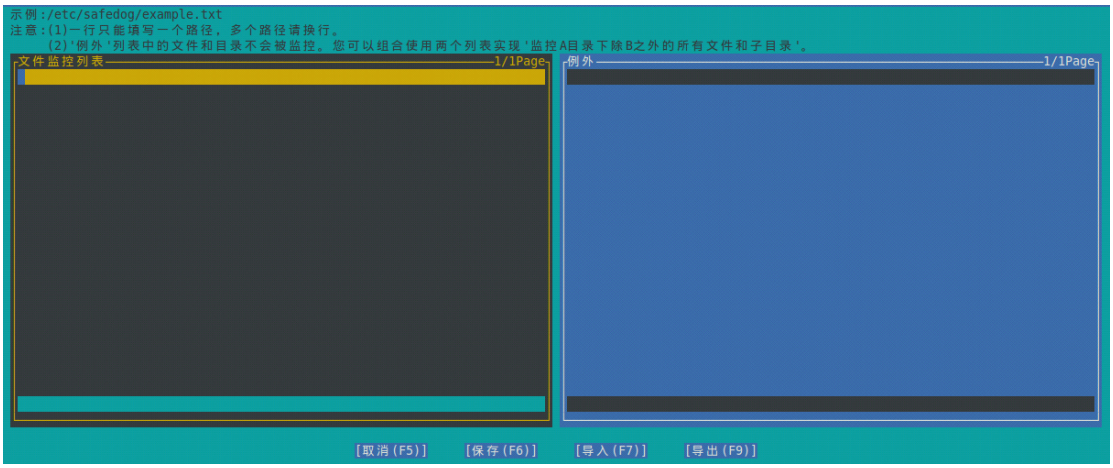


图 5.4.2 文件监控-文件监控列表

- 支持添加、修改、删除监控文件或目录等常规操作。
- 例外：支持设置文件和目录的监控白名单，此列表内的内容不被监控。可以组合设置，实现监控 A 目录下的除 B 之外的所有文件和目录。
- 设置特定路径，导入或导出文件监控列表。

注意：

- 会递归监控到子目录里面，当文件名列表为空时无法启动监视器。
- 禁止监控“/etc/safedog/monitor”这个目录及目录下的文件。
- 被监控的路径不能包含软链接或硬链接。
- 对文件或目录的描述请用绝对路径。
- 导入文件监控列表时，会覆盖已有的文件监控列表设置。
- 报告文件： **/etc/safedog/monitor/filemonit.txt**

5.4.2 进程监控

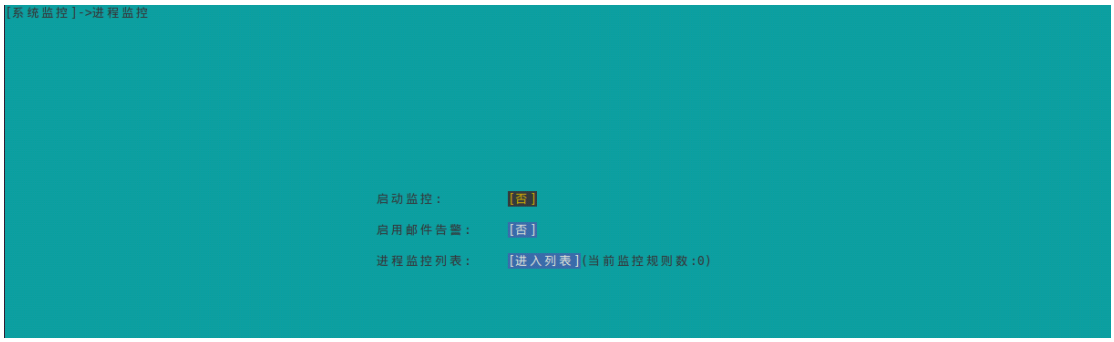


图 5.4.3 系统监控-进程监控

（1）启动监控：进程监控的功能开关。

（2）启用邮件告警：通过邮件发送监控记录给用户。此功能必须基于邮件告警相关信息已经成功设置，详见 5.5.5 章节。

（3）进程监控列表：列表列出所要监控的所有进程，支持添加、修改、删除监控进程。设置完进程名（必须包括运行参数）列表后，再开启监视器开关。

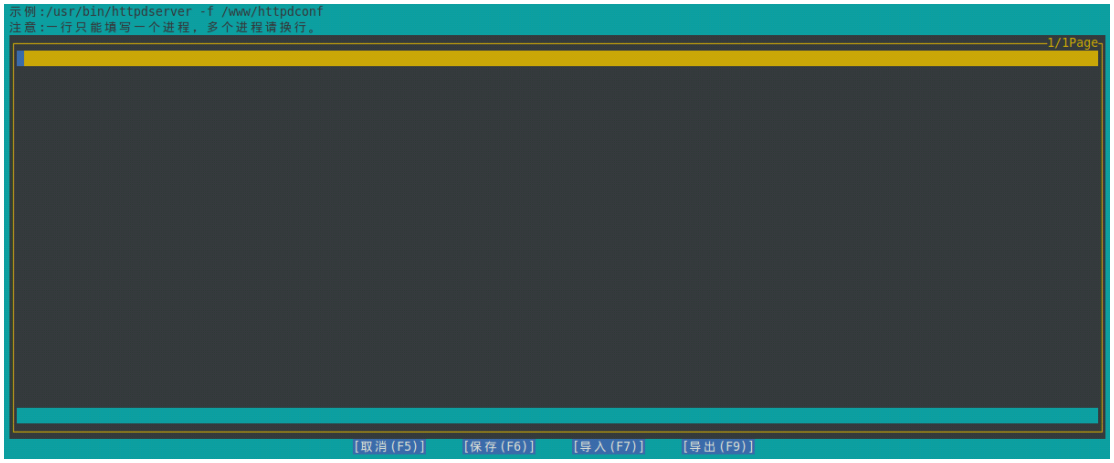


图 5.4.4 进程监控-进程监控列表

进程列表中的名字必须是绝对路径或者程序本身在 $PATH 环境变量表示的路径下，并且应该带上必须的启动参数。一旦检查到系统实时进程列表中没有该进程，会以所输入进程名作为命令执行重启进程的动作。

使用命令 **top** 或 **ps aux** 能够看到进程是否正在运行，一旦进程结束或被杀死，监视器会马上重启进程。

注意：

- 本功能只适用于监控可以通过一条命令启动的守护进程。
- 请对所设置的规则进行测试之后再启用，某些进程无法被监控，比如 apachectl

命令，实际启动的进程名字为 apache，这种情况下不适用本功能。

- 报告文件： **/etc/safedog/monitor/processmonit.txt**
- 当进程名列表为空时，无法启动监视器。

5.4.3 文件备份监控

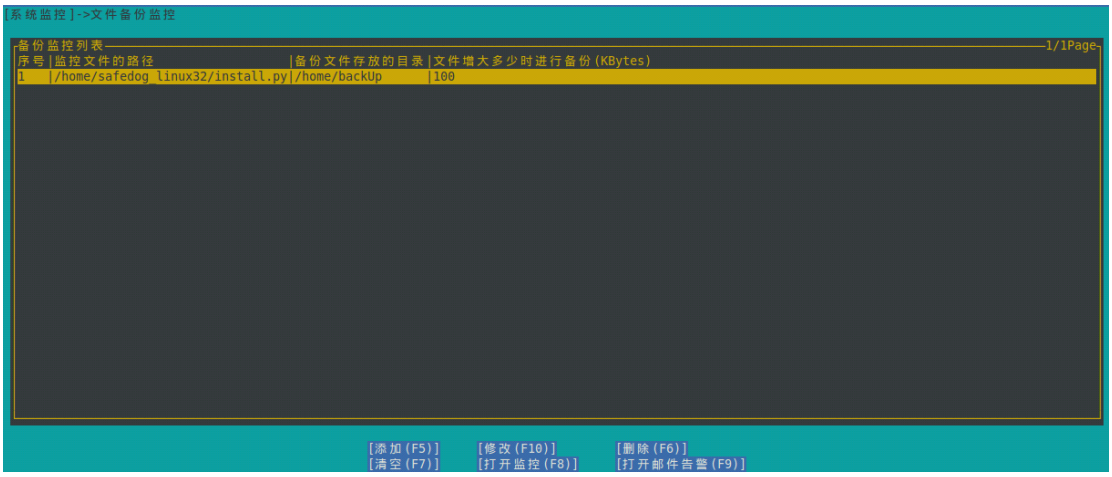


图 5.4.5 系统监控-文件备份监控

本功能适用于监控日志类的文件，该类文件会随着时间不停地增大。使用本功能可以在指定文件在增加多少体积时进行压缩备份。

（1）备份监控列表：显示所有正在监控的需要备份的文件信息。

（2）添加/修改：添加/修改备份文件。

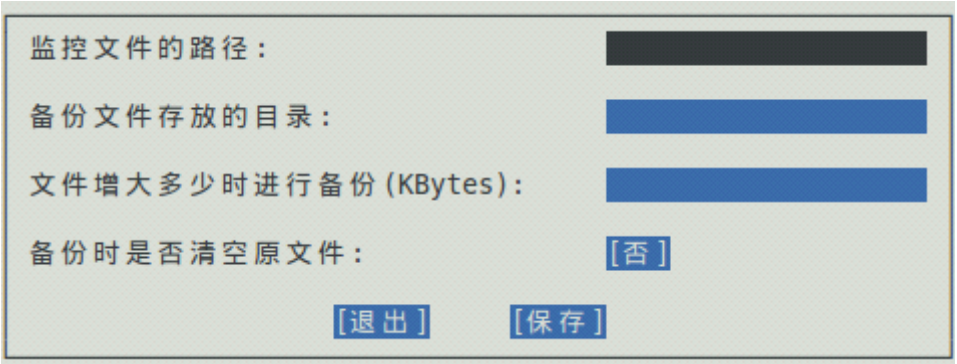


图 5.4.6 文件备份监控-添加

- 监控文件路径、备份文件存放的目录：填写绝对路径。
- 文件增大多少时进行备份：指定文件大小超过所设定值时，进行压缩备份到指定目录。
- 备份时是否清空原文件：若选择“是”，可以在备份的同时清空原文件，以避免原

文件体积过大影响性能。

（3）删除：删除所选监控文件。

（4）清空：删除所有监控文件。

（5）打开/关闭监控：文件备份监控的功能开关。

（6）打开邮件告警：通过邮件发送监控记录给用户。此功能必须基于邮件告警相关信息已经成功设置，详见 5.5.5 章节。

注意：

❖ 报告文件： **/etc/safedog/monitor/bakforsizemonit.txt**

5.4.4 CPU 监控

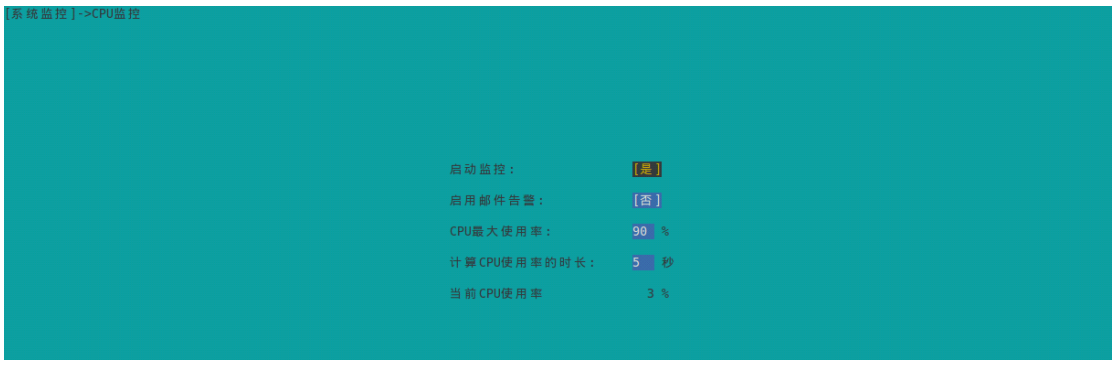


图 5.4.7 系统监控-CPU 监控

（1）启动监控：进程监控的功能开关。

（2）启用邮件告警：通过邮件发送监控记录给用户。此功能必须基于邮件告警相关信息已经成功设置，详见 5.5.5 章节。

（3）CPU 最大使用率：当 CPU 使用率超过该值时，在报告文件中记录监控信息。

（4）计算 CPU 使用率的时长：1-999 秒，该参数设定会在很大程度上影响计算结果，请合理设置，推荐设置 2-10 秒内，强烈建议不要超过 60 秒。

（5）当前 CPU 使用率：实时显示当前 CPU 使用率。

注意：

❖ 设置完监视范围后，再开启监视器开关。

❖ 报告文件：**/etc/safedog/monitor/cpumonit.txt**

5.4.5 内存监控

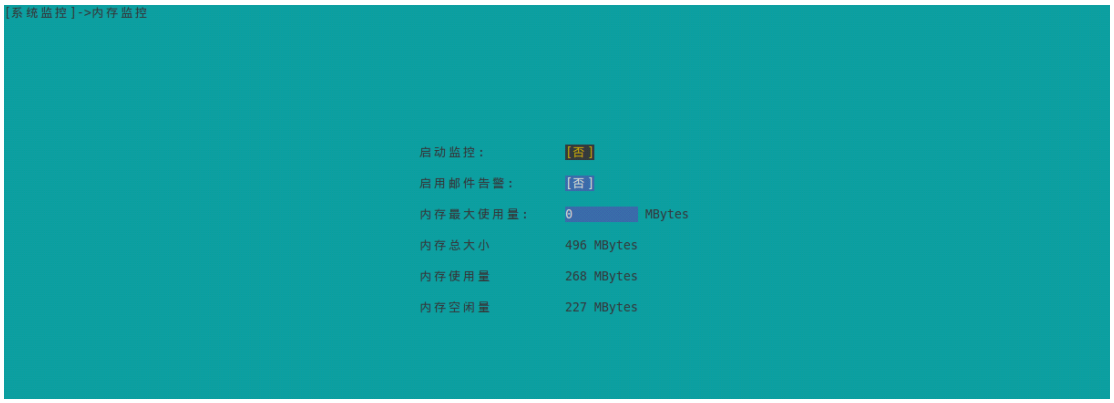


图 5.4.8 系统监控-内存监控

（1）启动监控：内存监控的功能开关。

（2）启用邮件告警：通过邮件发送监控记录给用户。此功能必须基于邮件告警相关信息已经成功设置，详见 5.5.5 章节。

（3）内存最大使用量（MBytes）：当内存使用量超过该值时，会在报告文件中记录监控信息。

（4）内存总大小（MBytes）：当前内存总大小。

（5）内存使用量（MBytes）：当前内存使用量。

（6）内存空闲量（MBytes）：当前内存空闲量。

注意：

- 设置完监视范围后，再开启监视器开关。
- 报告文件：**/etc/safedog/monitor/memorymonit.txt**

5.4.6 磁盘容量监控

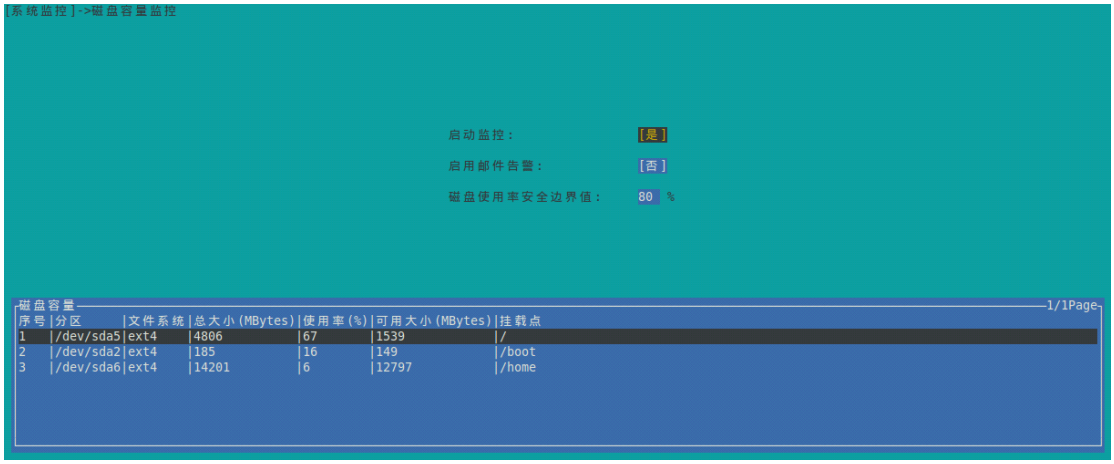


图 5.4.9 系统监控-磁盘容量监控

（1）启动监控：内存监控的功能开关。

（2）启用邮件告警：通过邮件发送监控记录给用户。此功能必须基于邮件告警相关信息已经成功设置，详见 5.5.5 章节。

（3）磁盘使用率安全边界值：当磁盘的某个分区的使用率超过了该百分比值，将在报告文件中记录监控信息。

（4）磁盘容量列表：显示所有磁盘的所有分区的使用率等信息。

注意：

- 设置完监视范围后，再开启监视器开关。
- 报告文件： **/etc/safedog/monitor/ diskvolumemonit.txt**

5.4.7 网络流量监控

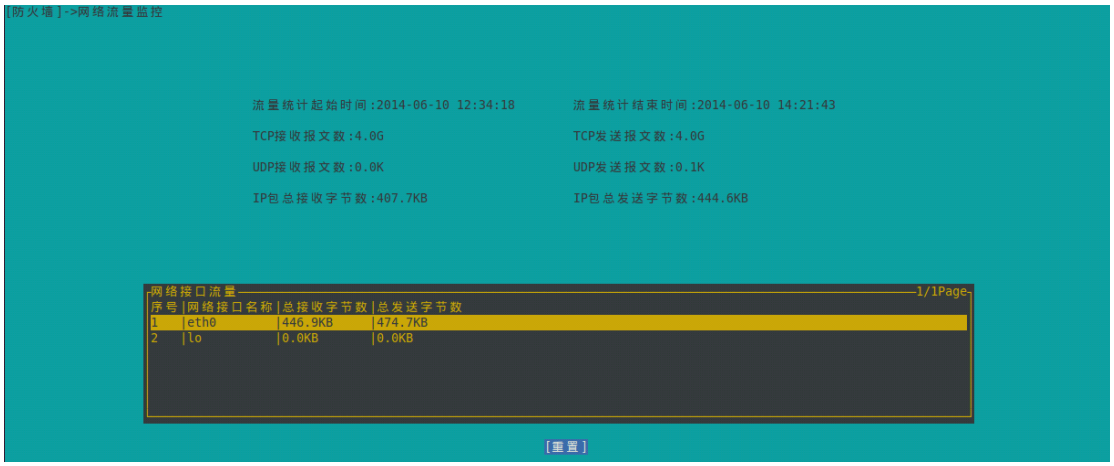


图 5.2.10 防火墙-网络流量监控

实时地展示了网络数据流量的统计结果。

（1）“起始时间”和“结束时间”：界面上所有流量数据的统计起止时间。

（2）重置：将所有的统计结果全部清零，从当前时刻开始重新统计。

注意：收发报文数与字节数的区别：

- 收发报文数不是字节数；
- IP 收发字节数统计各个网卡的 IP 包的数据总和；
- 各个网卡的收发字节数包含 IP 包与非 IP 包数据；
- 浏览统计结束时间表示当前时间，会自动更新；
- 重置按钮清零所有统计数据并将统计开始时间置为当前时间。

5.5 系统配置

5.5.1 系统状态配置

图 5.5.1 系统配置-系统状态配置

显示和修改系统状态信息，本菜单下每隔二到三秒会自动刷新状态。

（1）修改主机名：主机名不能输入空格且最大长度为 32 个字符。

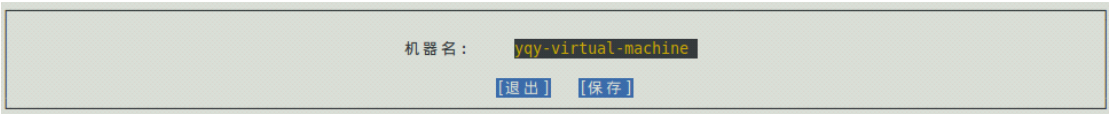


图 5.5.2 系统状态配置-修改主机名

（2）修改系统日期：

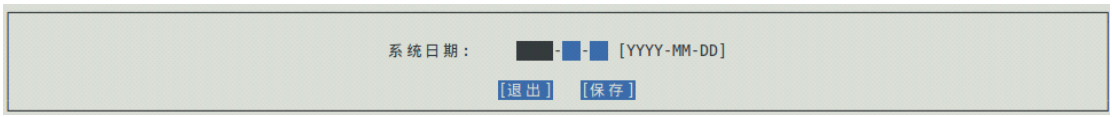


图 5.5.3 系统状态配置-修改系统日期

（3）修改系统时间：按照 24 小时制一次输入时分秒。

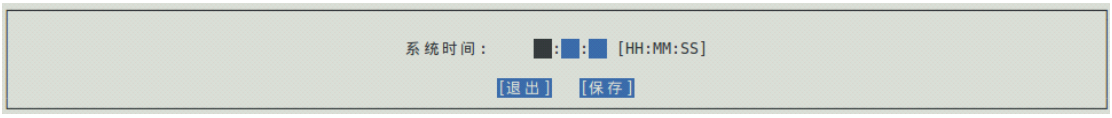


图 5.5.4 系统状态配置-修改系统时间

5.5.2 网络优化

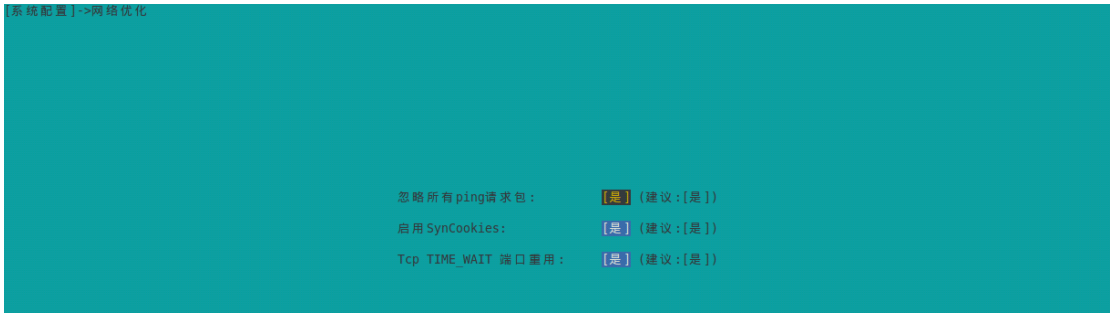


图 5.5.5 系统配置-网络优化

（1）忽略所有 ping 请求包：建议开启，开启时不响应 ping 请求，即任何主机无法 ping 通本机器。

（2）启用 SynCookies：建议开启，开启后对防范 syn flood 攻击有一定效果

（3）Tcp TIME_WAIT 端口重用：建议开启，开启后使处于 TIME_WAIT 状态的 TCP 端口允许被绑定。

5.5.3 资源优化

图 5.5.6 系统配置-资源优化

（1）最大共享内存：单个共享内存段的最大值。该值应该足够大，如果该值较小，建议调高。

（2）共享内存总大小限制（页）：所有共享内存总和的最大值。该值应该足够大。另外，页的大小可参考命令 `PAGESIZE` 。

（3）共享内存段最大个数：共享内存段的最大个数，该值应该足够大。

（4）最大线程个数：限制系统中所有进程的总线程个数最大值，系统进程数小于或者等于该值。该值应该足够大，通过软件设置该值应该不小于 512，否则设置失败。

（5）可分配的文件句柄最大个数：系统的文件描述符最大个数。该值应该足够大，通过软件设置该值应该不小于 4096，否则设置失败。

注意：

- 如果您不清楚本页面各个参数的功能，请不要进行修改。

5.5.4 邮件告警

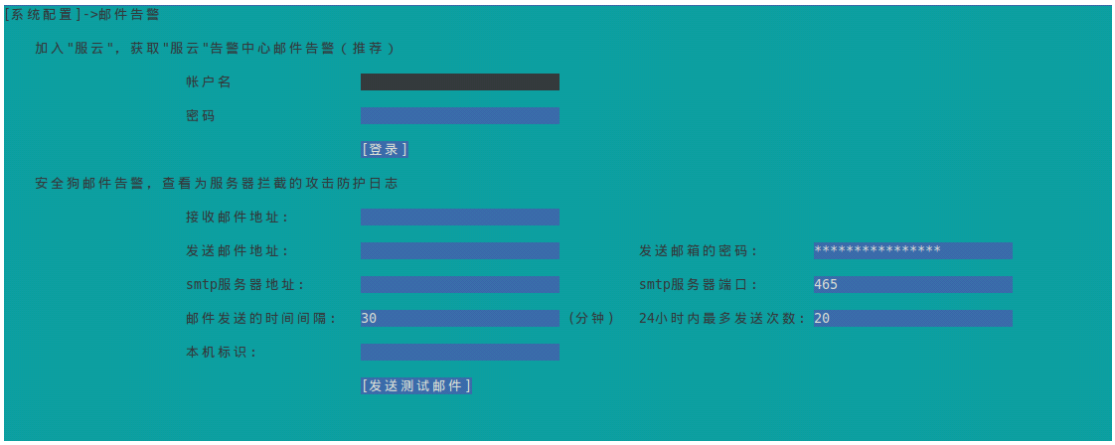


图 5.5.7 系统配置-邮件告警

通过配置并开启邮件告警功能，用户能够收到定期发送的服务器实时运行情况邮件，及时发现服务器异常。提供服云和安全狗告警两种方式。

（1）服云告警：输入用户名和密码后，自动下载用户证书，将服务器自动加入服云，出现如图 5.5.8 所示，此时即可登录服云体验服云告警功能。

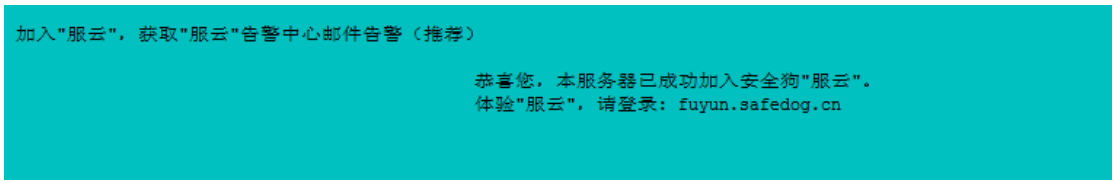


图 5.5.8 系统配置-服云告警

（2）安全狗告警：设置用于发送和接收邮件报告邮箱的参数，将系统监控的信息自动发送到接收邮箱。

- 接收邮件地址
- 发送邮件地址
- Smtp 服务器端口
- 发送邮箱的密码
- 邮件发送的时间间隔
- 本机标识
- 24 小时内最多发送次数：从设置时刻开始算起，每次重新设置该值都会重置起始时刻和邮件计数。
- 发送测试邮件：设置完以上参数后，可以尝试发送测试邮件。如果能够在接收邮箱里面收到测试邮件，表明设置正确且工作正常，否则可能是设置有错或者是网络工作不正常。目前可以支持 smtp 的邮件发送协议。

注意：

- 请确保邮件告警参数设置正确，否则在其他页面上都不能成功开启邮件告警。

5.6 应用程序配置

5.6.1 Iptables

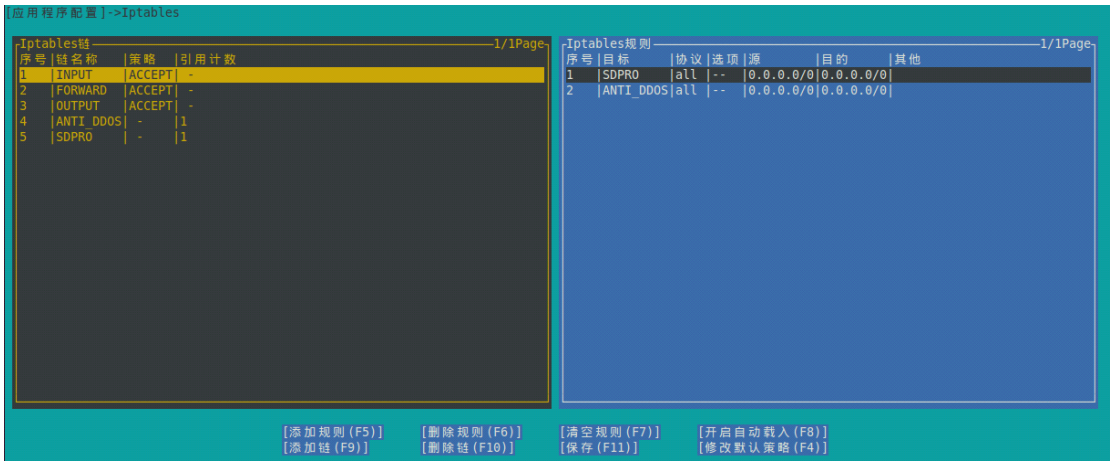


图 5.6.1 应用程序配置-Iptables

设置 IP 包过滤规则的系统，Linux 内核会根据 iptables 设定的规则对 IP 包进行过滤，从而构建成防火墙。

（1）Iptables 链：iptalbes 可以设置多个表，每个表包括多条链，每条链下面包含多条规则。本软件针对 iptables 中最主要的一个表 filter 进行显示和设置。

（2）Ipatables 规则：显示选中的 iptables 链对应的一组规则。

（3）添加规则：针对选中的 iptables 链，增加一组规则。

图 5.6.2 Iptables-增加规则

（4）删除规则：删除当前选中的 iptables 规则。

（5）清空规则：删除所有 iptables 规则。

（6）开启/关闭自动载入：**谨慎使用**自动载入功能，使用前确保当前的所有 iptables 规则是合理的，并且保存规则时未开启 DDOS 防护、SSH 登录拦截以及安全策略等功能，否则在重新启动时可能导致无法连上服务器或 iptables 异常。

（7）添加链：

图 5.6.3 Iptables-增加链

（8）删除链：删除当前选中的 iptables 链，对应的 iptables 规则也将删除。

（9）保存：保存修改。

（10）修改默认策略：修改当前选中的 ipables 链的策略，即 ACCEPT 或者 DROP。

注意：

- 不支持修改规则。若需要修改规则，需要先删除后增加规则。
- iptables 在系统重启后需要重新配置，除非启用了自动载入功能，并且手动保存过 iptables 表。

5.6.2 Vsftpd

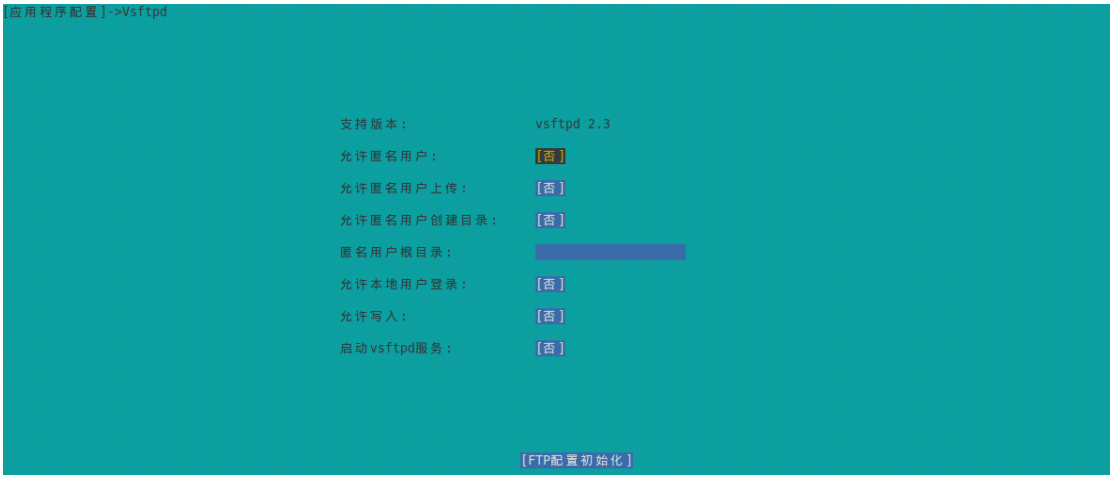


图 5.6.4 应用程序配置-Vsftpd

对系统中已安装未配置过的 vsftpd 进行一些简单的配置。

（1）支持版本

（2）允许匿名用户：是否允许匿名用户访问 FTP 服务器。

（3）允许匿名用户上传：是否允许匿名用户上传文件。

（4）允许匿名用户创建目录：是否允许匿名用户创建目录。

（5）匿名用户根目录：匿名用户登录时的目录。

（6）允许本地用户登录：是否允许本地用户（即用系统非 root 帐号和密码）访问 FTP 服务器。

（7）允许写入：是否允许登录的用户具有写权限，可用来全局禁止写权限。

（8）启动 vsftpd 服务：“是”，执行启动 FTP 服务器命令；“否”，执行关闭 FTP 服务器命令。

（9）FTP 配置初始化：使用本功能前须先初始化。

注意：

❖ 本软件只能对 vsftpd 进行简单的配置，如果需要更加复杂的设置，请直接参考 vsftpd 手册编辑。

❖ 使用本功能时，必须先对配置进行初始化。初始化以后，vsftpd 之前的配置信息会丢失，同时，匿名用户的根目录设置为/srv/ftp。通过软件配置完毕后，要使用配置生效，需要重启 ftp 服务。

❖ 配置完成后启动 vsftpd，然后通过网络访问本机的 ftpd 服务器测试配置项是否生效。

5.6.3 Samba

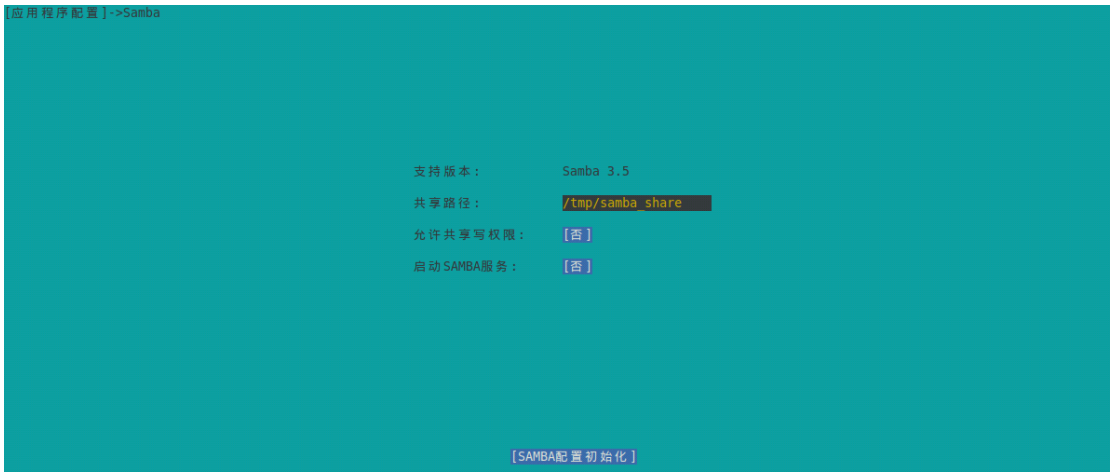


图 5.6.5 应用程序配置-Vsftpd

对系统中已安装未配置过的 samba 进行一些简单的配置。

（1）支持版本

（2）共享路径：共享文件夹路径。

（3）允许共享写权限：是否允许匿名用户写入共享文件夹。

（4）启动 SAMBA 服务：samba 服务的功能开关。

（5）SAMBA 配置初始化：使用本功能前须先初始化。

注意：

- 参考 vsftpd 的注意事项。

6. 软件卸载

在由安装包解压出来的目录下执行命令：

```
chmod +x uninstall.py
./uninstall.py
```

即可。

7. FAQ

7.1 Q:软件无法安装，提示如下：

```
sdsvrd: error while loading shared libraries:
/usr/lib/safedog/libcmdprosvr.so: cannot restore segment prot after reloc:
Permission denied
```

A：配置 selinux 权限允许软件安装和运行，或者关闭 selinux 服务。

7.2 Q:软件无法安装，提示：

```
need ... to install safedog for linux.
```

A：系统版本过老或者系统某些文件丢失，无法安装服务器安全狗。如果提示的文件确认已经存在，比如 iptables 程序在/sbin/目录下，但是仍然提示找不到。需要将该目录加入到 PATH 环境变量下。具体做法是修改/etc/profile，在文件的最后面加上一行

PATH=$PATH:/sbin

然后重启系统后，再重新安装即可。

7.3 Q:系统重启后功能失效

A：软件所有监控会在安全狗服务被关闭或重启后停止，请在重启服务或系统后重新进入 sdui 打开相关监控和功能。

7.4 Q:执行 sdui 时一直卡住，无法弹出界面，只能 ctrl+c 结束掉。

A：请等待一段时间，可能在执行任务过程中。如果几分钟后仍然没反应，执行 sdstart 重启安全狗服务，同时向我们报告 bug 现象。

7.5 Q: 配置 vsftpd 后，匿名用户登录后无法创建文件夹和上传文件。

A：首先，确认配置的时候开启了相关的权限；然后，匿名用户登录后的根目录是只读的，只能下载不能修改和删除。在根目录下的 upload 目录是里面可以实现创建文件夹和上传文件，但是不能修改和删除。

7.6 Q: service safedog start 出现提示 unrecognized service

A：请使用命令 sdstart 重启 safedog 服务。

7.7. Q: 软件功能部分失效。

A：检查 selinux 是否开启。需要关闭 selinux 才能正常运行本软件，如果您的 selinux 正在运行，则运行安全狗的时候可能会因为诸多权限被限制而出错，这时选可以选择设置 selinux 开放相关权限，或者关闭 selinux，要检查 selinux 状态可以使用"getenforce"命令查看，要关闭 selinux 可以使用命令"setenforce 0"。如果不是 selinux 的问题，请提交 bug 详情给我们，并提交相关日志信息，谢谢！

7.8 Q: 软件安装过程中在打印出" start initializing configuration, please wait seconds ..." 之后或卸载过程中卡住。

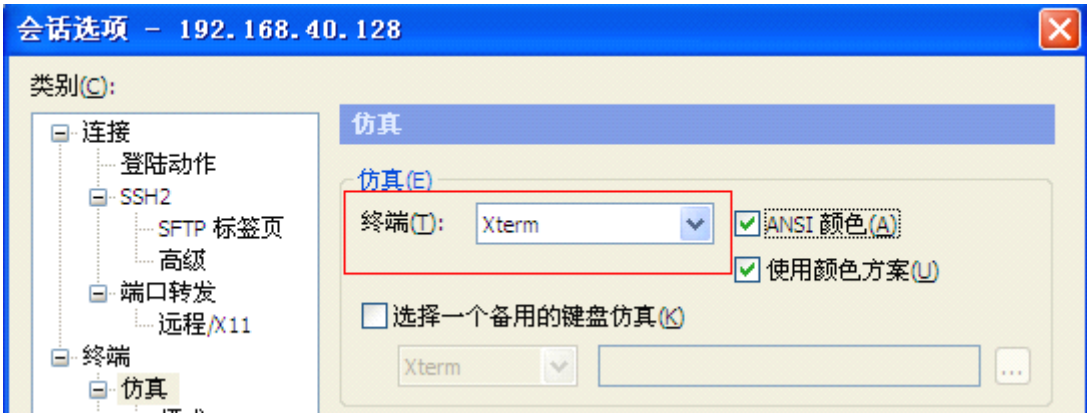
A：服务器由于网络原因连接不上升级中心，耐心等待 3~5 分钟，会跳过此步骤，继续完成后面的安装或卸载。如果已经手动中断了，要重新运行安装或卸载脚本。

7.9 Q: 使用 SecureCRT 运行 sdui 时报错：Error! Ncurses's initializition was failed!Please

replace the ssh terminal with xshell,putty or SecureCRT.

A：这个是由于终端类型不匹配引起的，请按照以下步骤操作：

Step 1：依次选择“选项”->“会话选项”->“终端”->“仿真”：



将终端类型修改为 Xterm。

Step2：将当前连接断开，再重新连接。

7.10 Q: 运行 sdui 时，画面没有颜色：

A：Step 1：依次选择“选项”->“会话选项”->“终端”->“仿真”：

把“ANSI 颜色”和“使用颜色方案”两 个打勾。

Step2：重启 SecureCRT。

8. 关于我们

8.1 关于我们

安全狗是国内知名的互联网安全品牌，专注于（云）服务器安全。首创的云+端云安全管理平台（SAAS 模式）为用户解决公有云、私有云和混合云环境中可能遇到的安全及管理问题，提供包含自动化系统风险识别和加固、系统级安全防护（防黑/防入侵/抗攻击）、云监控（安全监控/性能监控/日志监控）、云管理（多公有云管理/混合云管理）以及基于大数据架构的安全事件分析等功能。

安全狗云安全服务平台目前已经保护超过百万台的（云）服务器，日均为用户拦截超过千万次的攻击，是国内该领域用户量最大的云安全服务平台。

同时安全狗也积极参与到国内云计算安全生态的建设，目前已经跟国内主流大型云计算

平台建立合作伙伴关系；安全狗云安全服务平台已经成功对接各大云计算平台。

安全狗归属的厦门服云信息科技有限公司在成立不到两年时间内，获得了 IDG 等国内一线投资机构的 A、B 轮投资。作为一家年轻的云安全领域创业公司，我们致力于通过领先的安全技术、大数据处理平台为用户提供创新性的安全服务。

8.2 联系我们

8.2.1 官方网站

http://www.safedog.cn

8.2.2 官方论坛

http://bbs.safedog.cn

8.2.3 服务与支持

（1）在线支持： (工作日 8:40-18:00 非工作日：9:00-17:00)

（2）电话号码：0592-3775560 0592-3775561

（3）邮箱地址：tech@safedog.cn

8.2.4 市场与合作

（1）在线支持： (工作日 8:40-18:00 非工作日：9:00-17:00)

（2）电话号码：0592-3775556

（3）邮箱地址：web@safedog.cn

（4）联系地址：福建省厦门市软件园二期观日路 14 号

附表 命令行配置

1. 首页

1.1 系统体检

1. 自动体检开关

命令：sdcmd autoexam

参数：0/1

1.2 加入服云

1. 加入服云

命令：sdcloud -u 用户名

参数：服云帐号用户名

2. 查看加入服云命令

命令：sdcloud -h

参数：无

2. 防火墙

2.1 网络防火墙

2.1.1 DDOS 攻击防护

1.DDOS 开关

命令：sdcmd ddosflag

参数：0/1

2.IP 冻结时间

命令：sdcmd ddosdenytimelen

参数：时间长度（10-1000），单位分钟

3.TCP 端口数

命令：sdcmd portmax

参数：tcp 端口个数（2-1000）

4.TCP 请求数

命令：sdcmd syncountmax

参数：tcp 请求次数（1-268435455）

5.UDP 包个数

命令：sdcmd udpmax

参数：UDP 包最大个数（1-268435455）

6.ICMP 包个数

命令：sdcmd icmpmax

参数：icmp 包最大个数（1-268435455）

2.1.2 CC 攻击防护

1.CC 开关

命令：sdcmd webflag

参数：0/1

2.web 端口号

命令：sdcmd webport

参数：端口号，多个端口号之间用英文逗号隔开

例子：【sdcmd webport 80,8080】

3.URL 白名单

命令：sdcmd ddosurlwhite
参数：白名单的 URL 列表
例子：【sdcmd ddosurlwhite /discuz/index.php /discuz/data/1.jpg /date/image】

4.同一 URL 请求次数

命令：sdcmd urlsameuri
参数：最大请求次数（2-268435455）

5.代理个数

命令：sdcmd proxyipmax
参数：最大代理个数（0-268435455）

6.会话验证开关

命令：sdcmd verifyflag
参数：0/1

7.会话验证模式

命令：sdcmd verifyfirstflag
参数：0/1
（1 表示对所有访问 IP 都进行验证， 0 表示仅对判定为 CC 攻击的 IP 进行验证）

8.验证失败次数

命令：sdcmd verifymax
参数：次数（2-99）

9.IP 冻结时间

命令：sdcmd ccdenytime
参数：时间长度（10-1000），单位分钟

2.1.3 安全策略

1.安全策略开关

命令：sdcmd ssflag
参数：0/1

2.添加安全策略

命令：sdcmd addss
参数：共有 4 个参数，依次为“协议”，“端口”，“策略”，“例外 IP”
协议：1 表示 tcp；2 表示 udp； 3 表示 icmp；4 表示 igmp
端口：tcp 或 udp 端口号，若“协议”不是 tcp 或 udp，则设为 0
策略：1 表示 Accpet；2 表示 Drop
例外 IP：多个 ip 地址之间用英文逗号隔开
例子：
除了 110.123.1.2 和 182.12.14.46 外，所以 IP 都禁止访问 tcp 端口 3453【sdcmd addss

1 3453 2 110.123.1.2,182.12.14.46】

除了 110.123.1.2 外，所有 IP 都禁止 ping 本服务器【sdcmd addss 3 0 2 110.123.1.2】

3.删除某条安全策略规则

命令：sdcmd rmss

参数：安全策略规则的 ID 号（ID 号从 0 开始计数，即最小的 ID 应该是 0，而不是 1）

注意：在 sdui 界面上，安全策略规则列表中，每条规则前有个"序号"，该序号是从 1 开始计数的。所以，ID 号和序号的关系是：ID=序号-1

4.清空安全策略规则

命令：sdcmd clrss

参数：无

5.修改某条安全策略规则

命令：sdcmd modss

参数：共有 5 个参数：依次为“要修改的策略规则序号”，“协议”，“端口”，“策略”，“例外 IP”

要修改的策略规则序号：从 0 开始

其他四个参数的说明见“2. 添加安全策略”

2.1.4 暴力破解防御

1.FTP 防暴力破解

（1）开关

命令：sdcmd ftpflag

参数：0/1

（2）FTP 端口

命令：sdcmd ftpport

参数：端口号，多个端口号之间用英文逗号隔开

例子：【sdcmd ftpport 21】

（3）登录次数

命令：sdcmd ftppwdmax

参数：最大错误次数（3-100）

（4）IP 冻结时间

命令：sdcmd ftpdenytime

参数：时间长度（10-1000），单位分钟

2.SSH 防暴力破解

（1）开关

命令：sdcmd sshddenyflag

参数：0/1

（2）登录次数

命令：sdcmd sshdallowerrormax

参数：最大次数（1-99）

（3）IP 冻结时间

命令：sdcmd sshddenytimelen

参数：时间长度（10-1000），单位分钟

（4）SSH 立即解除拦截

命令：sdcmd sshdcanceldenyip

参数：IP 地址

例子：【sdcmd sshdcanceldenyip 110.10.23.2】

2.1.5 IP 黑名单

1.开关

命令：sdcmd superblackflag

参数：0/1

2.IP 黑名单列表

命令：sdcmd superblack

参数：IP（段）列表，以空格分隔多个

例子：【sdcmd superblack 1.2.3.4 111.111.0.0-111.111.255.255】

2.1.6 IP 白名单

1.开关

命令：sdcmd superwhiteflag

参数：0/1

2.IP 白名单列表

命令：sdcmd superwhite

参数：IP（段）列表，以空格分隔多个

例子：【sdcmd superwhite 1.2.3.4 111.111.0.0-111.111.255.255】

2.1.7 邮件告警

1.开关

命令：sdcmd ddosmail

参数：0/1

3. 主动防御

3.1 系统帐号保护

1. 系统帐号变动邮件报警开关

命令：sdcmd accountmail

参数：0/1

3.2 SSH 远程登录保护

1. SSH 端口号

命令：sdcmd sshport

参数：ssh 端口号

2. SSH 远程异地登陆提醒

命令：sdcmd sshdloginalarmflag

参数：0/1

3. 白名单访问控制开关

命令：sdcmd sshwhiteflag

参数：0/1

4. 登录日志邮件报警开关

命令：sdcmd loginmail

参数：0/1

5. SSH 远程登录白名单列表

命令：sdcmd sshwhite

参数：IP（段）列表，以空格分隔多个

例子：【sdcmd sshwhite 1.2.3.4 111.111.0.0-111.111.255.255】

4. 系统监控

4.1 文件监控

1. 文件监控开关

命令：sdcmd fmonitflag

参数：0/1

例子：设置为“是”【sdcmd fmonitflag 1】；设置为“否”【sdcmd fmonitflag 0】

2. 文件监控邮件报警开关

命令：sdcmd fmail

参数：0/1

例子：设置为“是”【sdcmd fmail 1】；设置为“否”【sdcmd fmail 0】

3. 文件监控列表

命令：sdcmd fmonitlist

参数：文件或目录的路径列表，以空格分隔

例子：【sdcmd fmonitlist /home/a.txt /homt/dirnew /var/log/mylog.log】

4.2 进程监控

1. 进程监控开关

命令：sdcmd pmonitflag

参数：0/1

2. 进程监控邮件报警开关

命令：sdcmd pmail

参数：0/1

4.3 CPU 监控

1. CPU 监控开关

命令：sdcmd cmonitflag

参数：0/1

2. CPU 监控邮件报警开关

命令：sdcmd cmail

参数：0/1

3. CPU 监控最大使用率

命令：sdcmd cceil

参数：使用率（1-99）
例子：设置最大使用率为 90%【sdcmd cceil 90】

4. 计算 CPU 使用率的时长

命令：sdcmd ccalctime
参数：时间长度（1-999），单位秒

4.4 内存监控

1. 内存监控开关

命令：sdcmd mmonitflag
参数：0/1

2. 内存监控邮件报警开关

命令：sdcmd mmail
参数：0/1

3. 内存最大使用量

命令：sdcmd mceil
参数：内存最大使用字节数，单位 MB

4.5 磁盘容量监控

1. 磁盘空间监控开关

命令：sdcmd dmonitflag
参数：0/1

2. 磁盘空间监控邮件报警开关

命令：sdcmd dmail
参数：0/1

3. 磁盘使用率安全边界值

命令：sdcmd diskpercent
参数：磁盘使用率（6-99），单位%

4.6 文件备份监控

1. 文件备份开关

命令：sdcmd bakforsizeflag
参数：0/1

2. 文件备份邮件报警开关

命令：sdcmd bfmail
参数：0/1

3. 添加文件备份规则

命令：sdcmd bakforsizeadd

参数：共有 4 个参数，参数间用空格隔开，依次为“监控文件的路径” “备份文件存放的目录” “文件增大多少 KB 进行备份” “备份时是否清空原文件，用 0/1 表示”

例子：

/var/test.log 增大 1024kB 时，将其备份到/home/backup 目录，并清空/var/test.log 文件：

【sdcmd bakforsizeadd /var/test.log /home/backup 1024 1】

4. 删除某个文件备份规则

命令：sdcmd bakforsizedel

参数：文件备份规则的序号

例子：删除第 3 条文件备份规则 【sdcmd bakforsizedel 3】

5. 清空所有文件备份规则

命令：sdcmd bakforsizeclr

参数：无

4.7 网络流量监控

1. 重置网络流量统计

命令：sdcmd resetflow

参数：无

5. 系统配置

5.1 网络优化

1. 忽略所有 ping 请求包

命令：sdcmd ping

参数：0/1

例子：设置为“是”【sdcmd ping 1】；设置为“否”【sdcmd ping 0】

2. 启用 SynCookies

命令：sdcmd tcpsyn

参数：0/1

例子：设置为“是”【sdcmd tcpsyn 1】；设置为“否”【sdcmd tcpsyn 0】

3. Tcp TIME_WAIT 端口重用

命令：sdcmd twreuse

参数：0/1

5.2 资源优化

1. 最大共享内存

命令：sdcmd shmmax

参数：字节数

2. 共享内存总大小限制

命令：sdcmd shmall

参数：字节数

3. 共享内存段最大个数

命令：sdcmd shmmni

参数：字节数

4. 最大线程个数

命令：sdcmd threadmax

参数：线程个数（512-99999）

5. 可分配的文件句柄最大个数

命令：sdcmd filemax

参数：文件句柄个数（4096-999999）

5.3 邮件告警

1. 接收告警的邮箱设置

命令：sdcmd mailrecvacc
参数：邮箱账号
例子：【sdcmd mailrecvacc abctest@xxx.xxx】

2. 发送告警的邮箱设置

命令：sdcmd mailsendacc
参数：邮箱账号
例子：【sdcmd mailsendacc testsendacc@yyy.yyy】

3. 发送告警的邮箱的服务器

命令：sdcmd mailsmtpserver
参数：服务器 IP 地址
例子：【sdcmd mailsmtpserver 123.123.123.123】

4. 发送告警的邮箱的服务器的端口号

命令：sdcmd mailsmtpport
参数：端口号
例子：【sdcmd mailsmtpport 465】

5. 发送告警的邮箱的密码

命令：sdcmd mailsendpwd
参数：邮箱账号的正确密码
例子：【sdcmd mailsendpwd mypasswd】
注意：特殊字符（如：“!”“@”“#”“$”等）前面需要加转义字符“\”

6. 告警邮件的最小间隔时间

命令：sdcmd mailintv
参数：分钟数
例子：【sdcmd mailintv 30】

7. 告警邮件中显示的机器名

命令：sdcmd mailmachinename
参数：机器名字符串
例子：【sdcmd mailmachinename host001】

8. 每日告警邮件最大数量

命令：sdcmd mailmaxperday
参数：邮件数
例子：【sdcmd mailmaxperday 20】

9. 发送测试邮件

命令：sdcmd mailtest

参数：无

6. 其他

1. 获取服务器安全狗的所有设置

命令：sdcmd check

参数：无