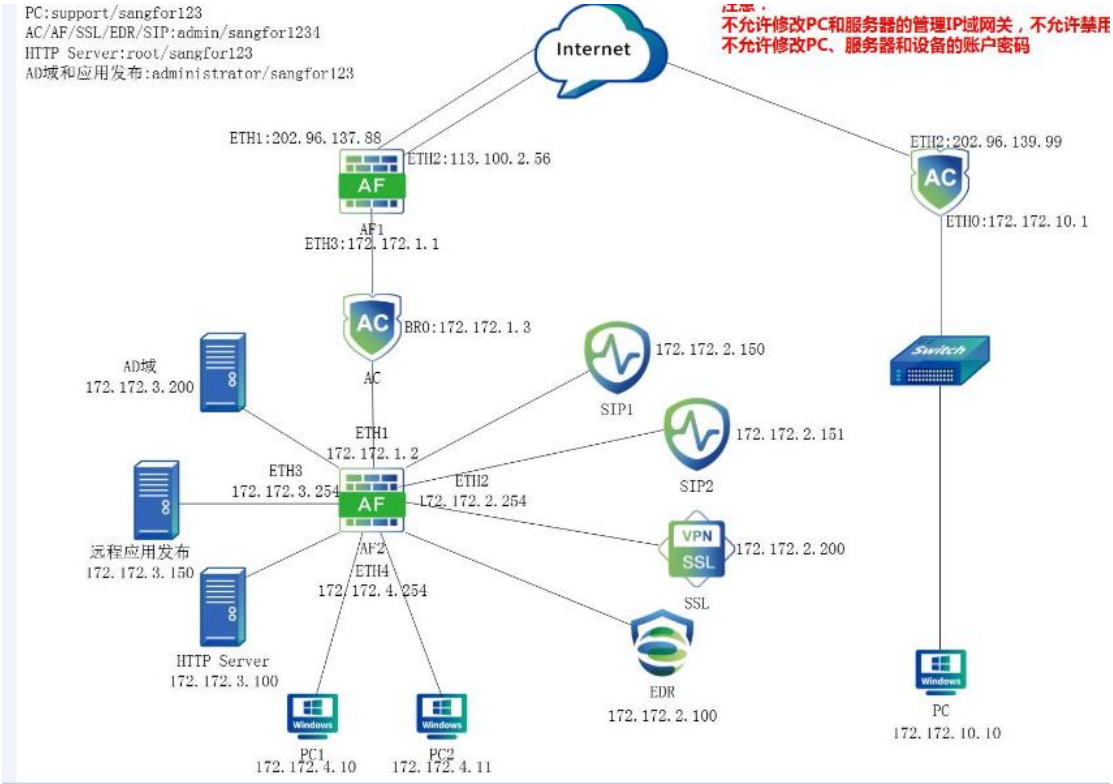
AC 配置实验

一、 实验环境如图:

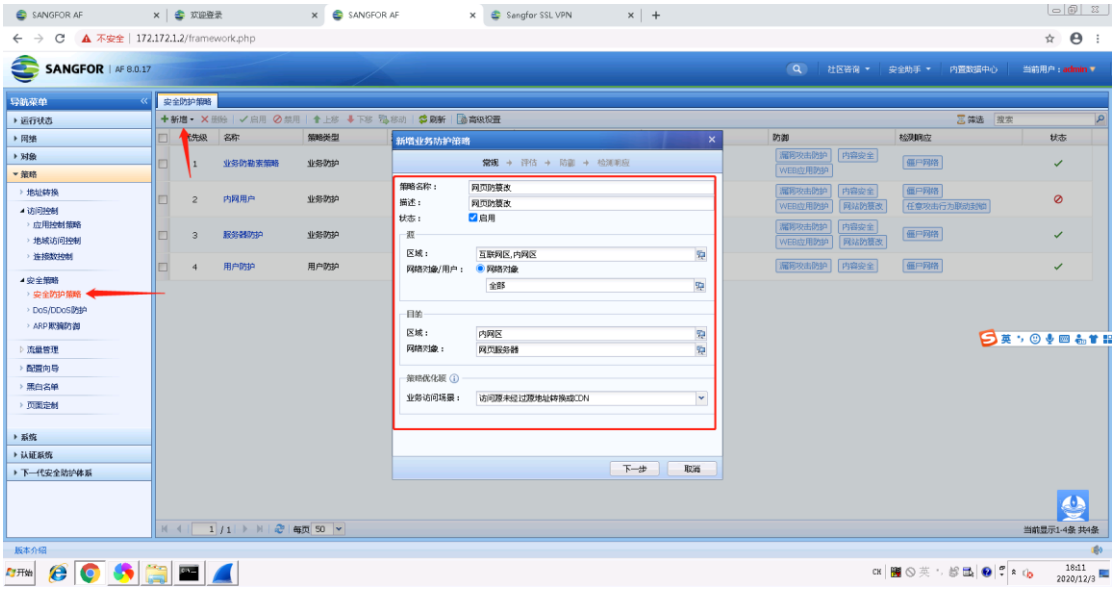


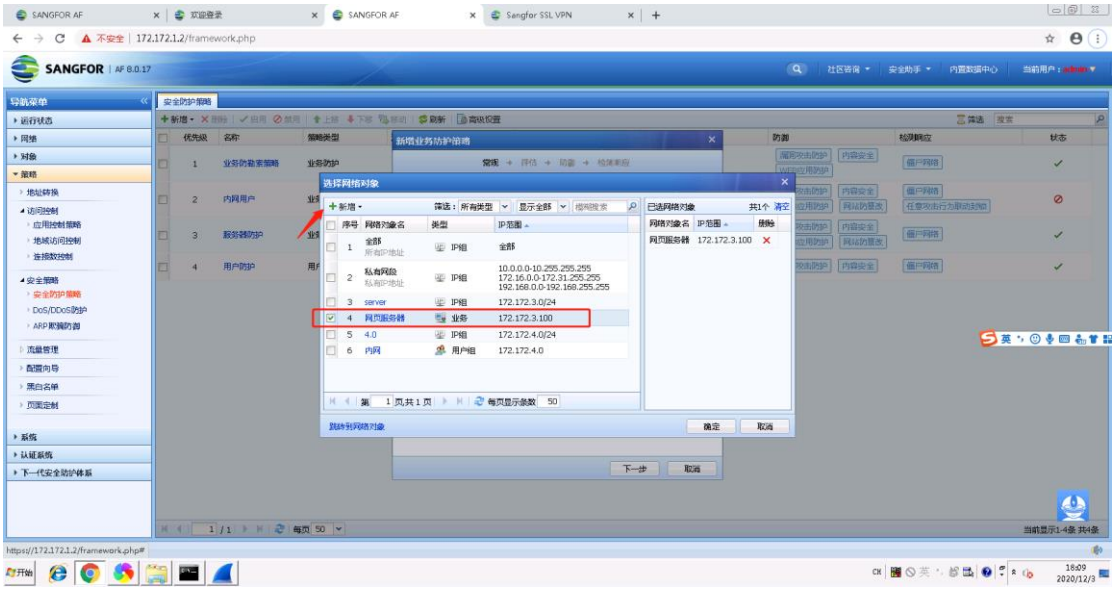
二、 实现要求:

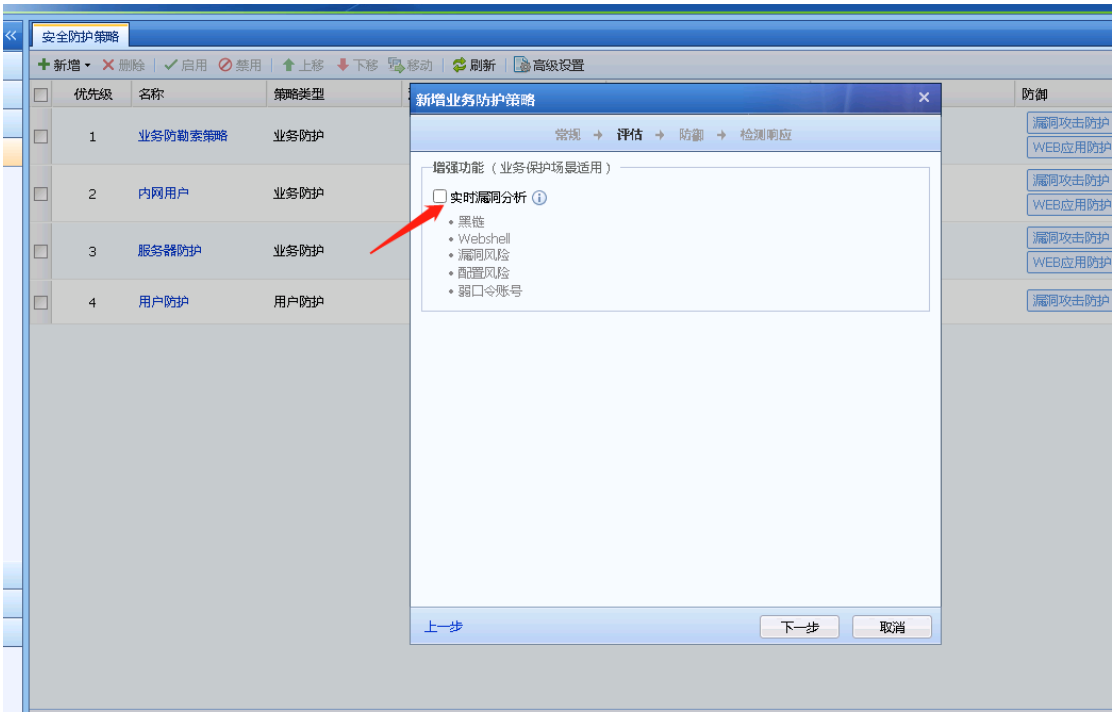
1、AF 网站防篡改;

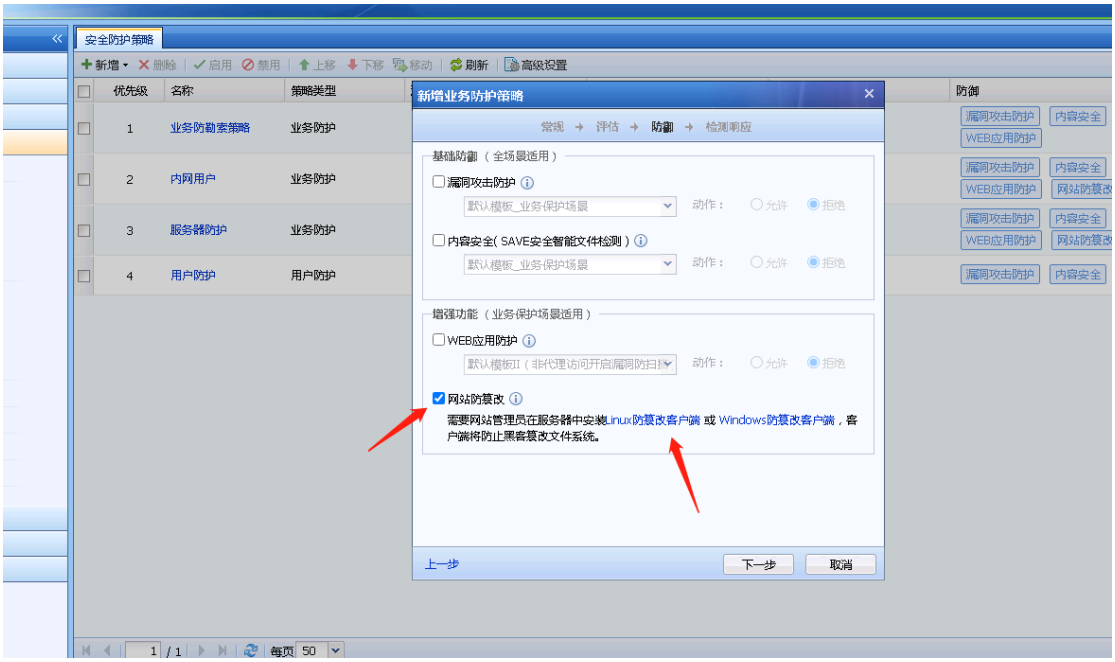
三、 实验步骤如下:

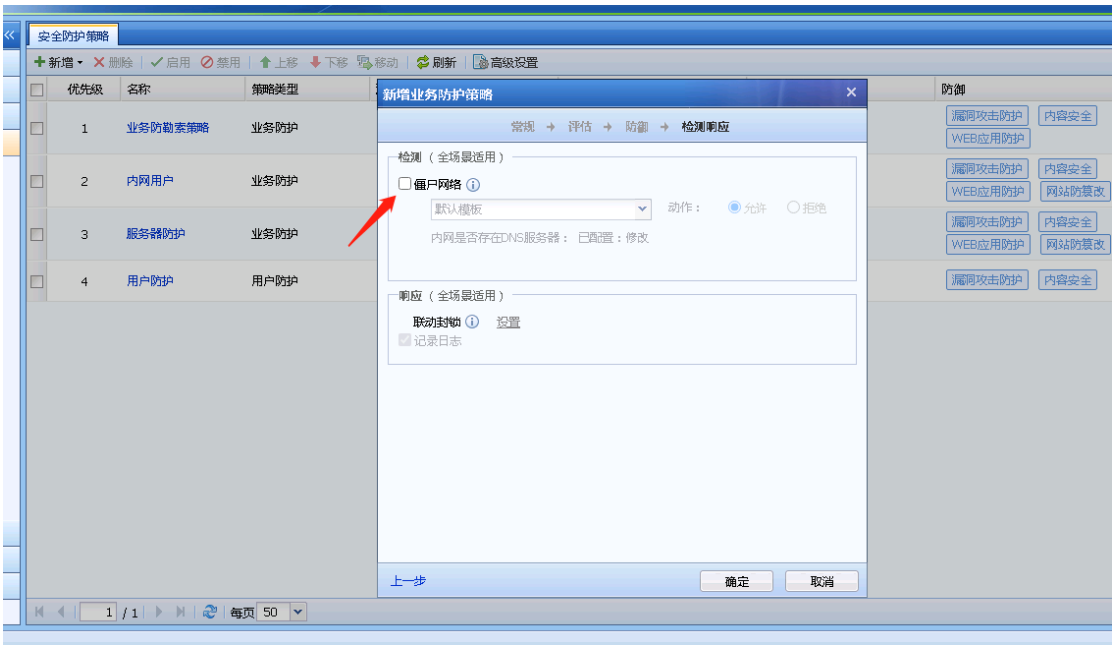
1、 登录 AF2 进行配置

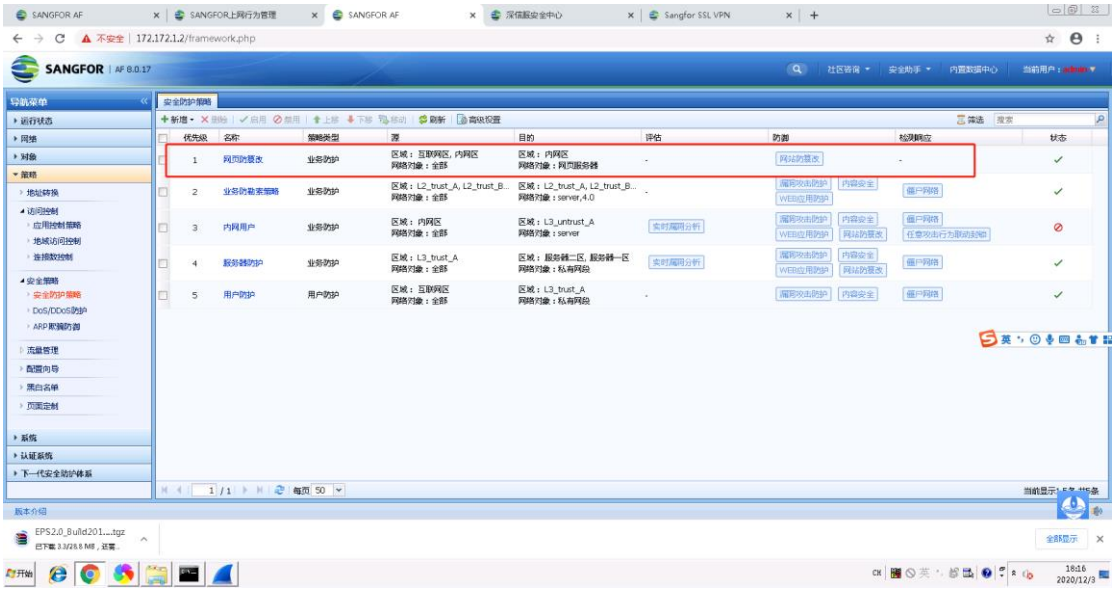

SANGFOR AF
SANGFOR SSL VPN
不安全 | 172.172.1.2/framework.php
SANGFOR | AF 8.0.17
导航菜单
安全防护策略
新增业务防护策略
网页防篡改
互联网区,内网区
全部
内网区
网页服务器
访问原来经过原地址转换成CDN
下一步
取消


SANGFOR AF
SANGFOR SSL VPN
不安全 | 172.172.1.2/framework.php
SANGFOR | AF 8.0.17
导航菜单
安全防护策略
新增业务防护策略
选择网络对象
网页服务器
172.172.3.100
确定
取消
下一步

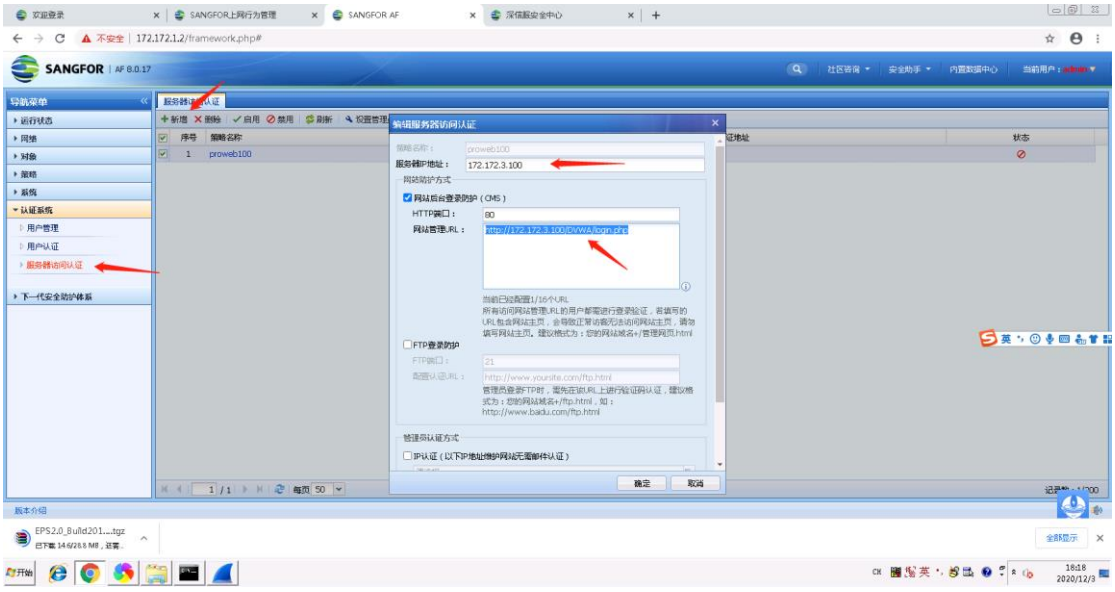

安全防护策略
新增
删除
启用
禁用
上移
下移
移动
刷新
高级设置
优先级
名称
策略类型
防御
1
业务防勒索策略
业务防护
2
内网用户
业务防护
3
服务器防护
业务防护
4
用户防护
用户防护
漏洞攻击防护
WEB应用防护
新增业务防护策略
常规
评估
防御
检测响应
增强功能（业务保护场景适用）
实时漏洞分析
黑链
Webshell
漏洞风险
配置风险
弱口令账号
上一步
下一步
取消

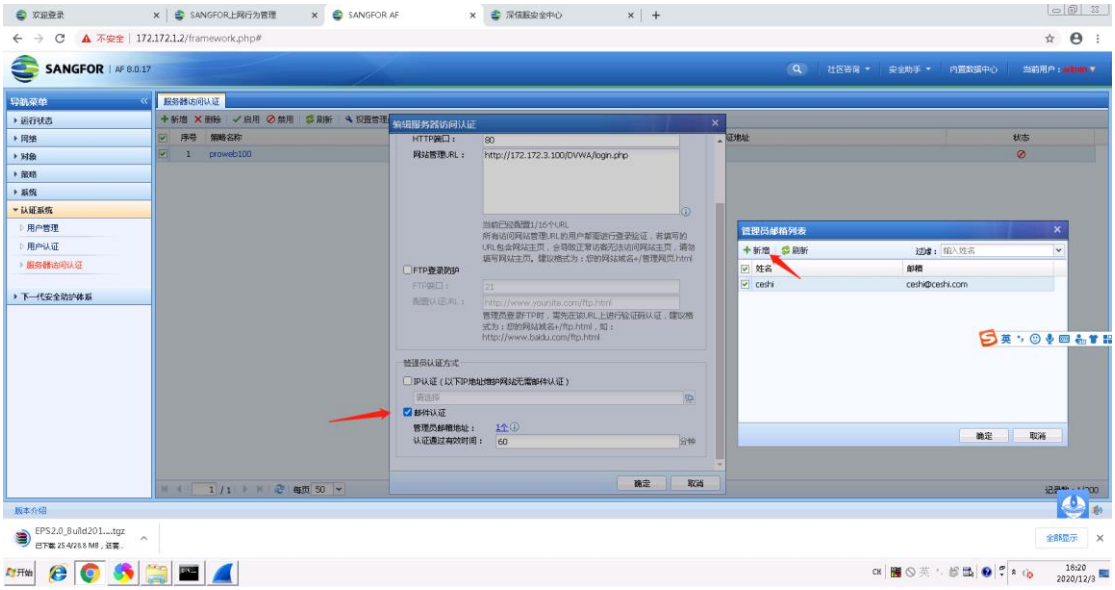

安全防护策略
新增
删除
启用
禁用
上移
下移
移动
刷新
高级设置
优先级
名称
策略类型
防御
1
业务防勒索策略
业务防护
2
内网用户
业务防护
3
服务器防护
业务防护
4
用户防护
用户防护
新增业务防护策略
常规
评估
防御
检测响应
基础防御（全场景适用）
漏洞攻击防护
默认模板_业务保护场景
动作：
允许
拒绝
内容安全（SAVE安全智能文件检测）
增强功能（业务保护场景适用）
WEB应用防护
网站防篡改
需要网站管理员在服务器中安装Linux防篡改客户端 或 Windows防篡改客户端，客户端将防止黑客篡改文件系统。
上一步
下一步
取消
每页 50

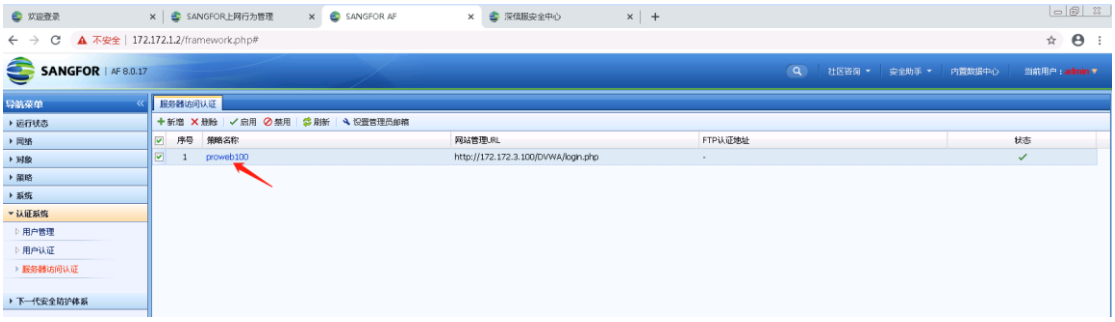

安全防护策略
新增
删除
启用
禁用
上移
下移
移动
刷新
高级设置
优先级
名称
策略类型
防御
1
业务防勒索策略
业务防护
2
内网用户
业务防护
3
服务器防护
业务防护
4
用户防护
用户防护
新增业务防护策略
常规
评估
防御
检测响应
检测（全场景适用）
僵尸网络
默认模板
动作：
允许
拒绝
内网是否存在DNS服务器：
已配置：修改
响应（全场景适用）
联动封锁
设置
记录日志
上一步
确定
取消
每页 50


SANGFOR
AF 8.0.17
安全防护策略

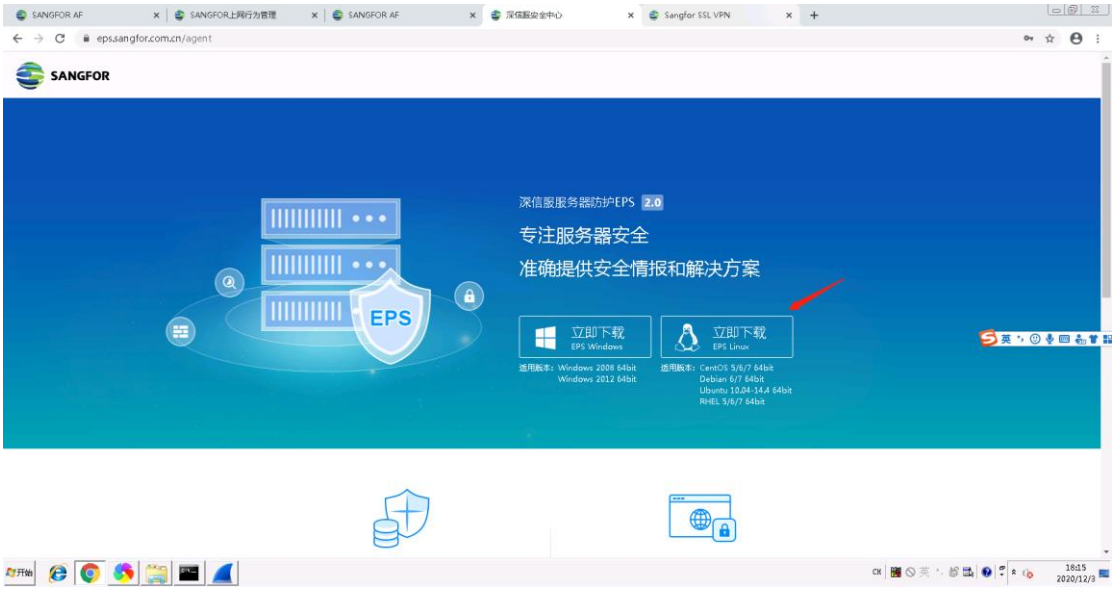
2、 配置认证系统



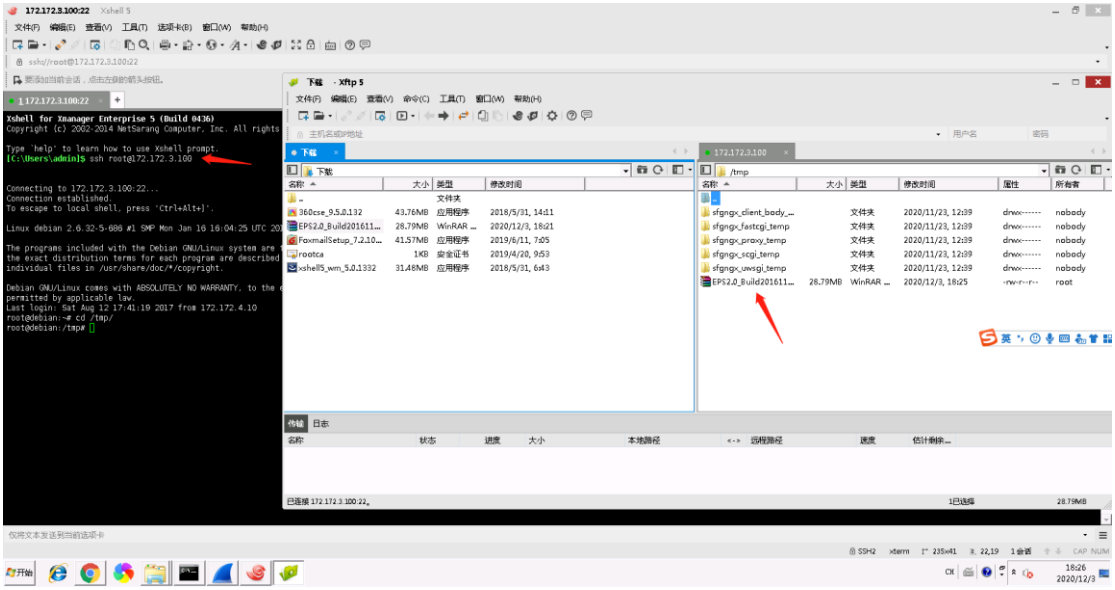




3、 下载防篡改客户端



使用 ssh 登录 Web 服务器，并将下载的安装包上传至服务器



检测服务器是否安装客户端，卸载原有安装包

卸载账号密码：admin/epsgreat888

给解压的安装包赋予执行权限，安装软件

```
root@debian:/usr# mkdir /usr/eps
root@debian:/usr# cd /tmp/
root@debian:/tmp# ./
agent_installer.bin      .ICE-unix/              sfgngx_client_body_temp/ sfgngx_fastcgi_temp/     sfgngx_proxy_temp/       sfgngx_scgi_temp/        sfgngx_uwsgi_temp/       .X11-unix/
root@debian:/tmp# ./agent_installer.bin /usr/eps/
eps agent is installing on x86 machines
extract eps_base.tgz
extract eps_packman.tgz
extract eps_sys.tgz
extract sfguard.tgz
/usr/eps/ install success
eps start success
root@debian:/tmp#
```

对 eps 软件进行配置

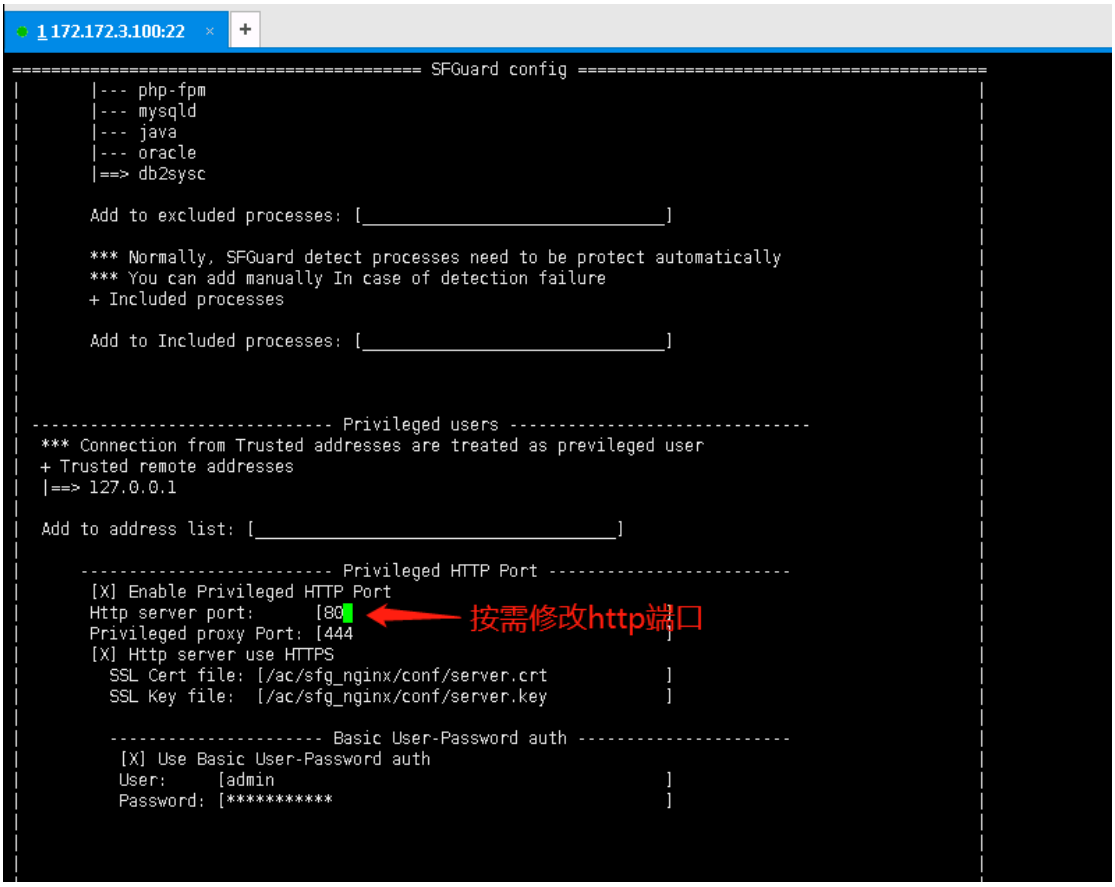
```
root@debian:/tmp# cd /usr/eps/
root@debian:/usr/eps# ls
agent_scripts  bin  config  lib  lmodules  lualibs  packages  services  var
root@debian:/usr/eps# cd bin/
root@debian:/usr/eps/bin# ./sfgconfig
```

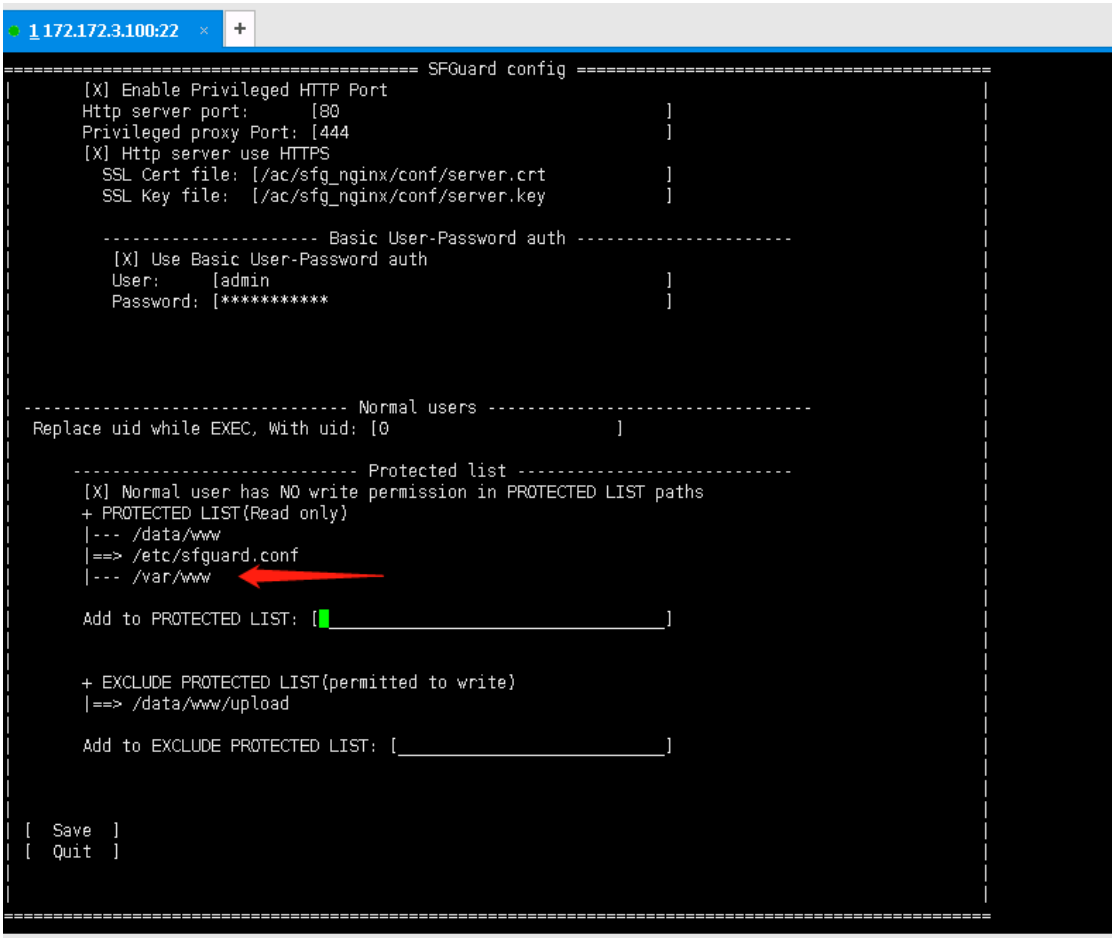
1 172.172.3.100:22

```
========================================= SFGuard config =========================================
|                                                                                                 |
|  ------------------------------ Global config --------------------------------                  |
|   Help:                                                                                         |
|      <Up>,<Down>,<Tab> to switch between input components                                       |
|      <Space>,<Enter> to toggle checkbox/button                                                  |
|      <Del> to delete item in list                                                               |
|      toggle [ Save ], [ Quit ] in the end of form to save or quit                               |
|                                                                                                 |
|    [X] Enable SFGuard system                                                                    |
|    [X] Log to Sangfor NGAF device                                                               |
|        Sangfor NGAF address: [172.172.3.254                          ]                          |
|        Guard Policy Name: [proweb100                                 ]                          |
|    [X] Trace granted operations                                                                 |
|        [X] Trace granted FileSystem operations only                                             |
|    [X] Trace EXEC syscalls                                                                      |
|                                                                                                 |
|        ------------------------- Process protection -------------------------                   |
|         + Excluded processes                                                                    |
|         |==> sfg_nginx                                                                          |
|         |--- apache2                                                                            |
|         |--- nginx                                                                              |
|         |--- httpd                                                                              |
|         |--- lloader                                                                            |
|         |--- php-fpm                                                                            |
|         |--- mysqld                                                                             |
|         |--- java                                                                               |
|         |--- oracle                                                                             |
|         |--- db2sysc                                                                            |
|                                                                                                 |
|         Add to excluded processes: [_____________________________]                              |
|                                                                                                 |
|         *** Normally, SFGuard detect processes need to be protect automatically                 |
|         *** You can add manually In case of detection failure                                   |
|         + Included processes                                                                   |
|                                                                                                 |
|         Add to Included processes: [_____________________________]                              |
|                                                                                                 |
|                                                                                                 |
-------------------------------------------------------------------------------------------------
```

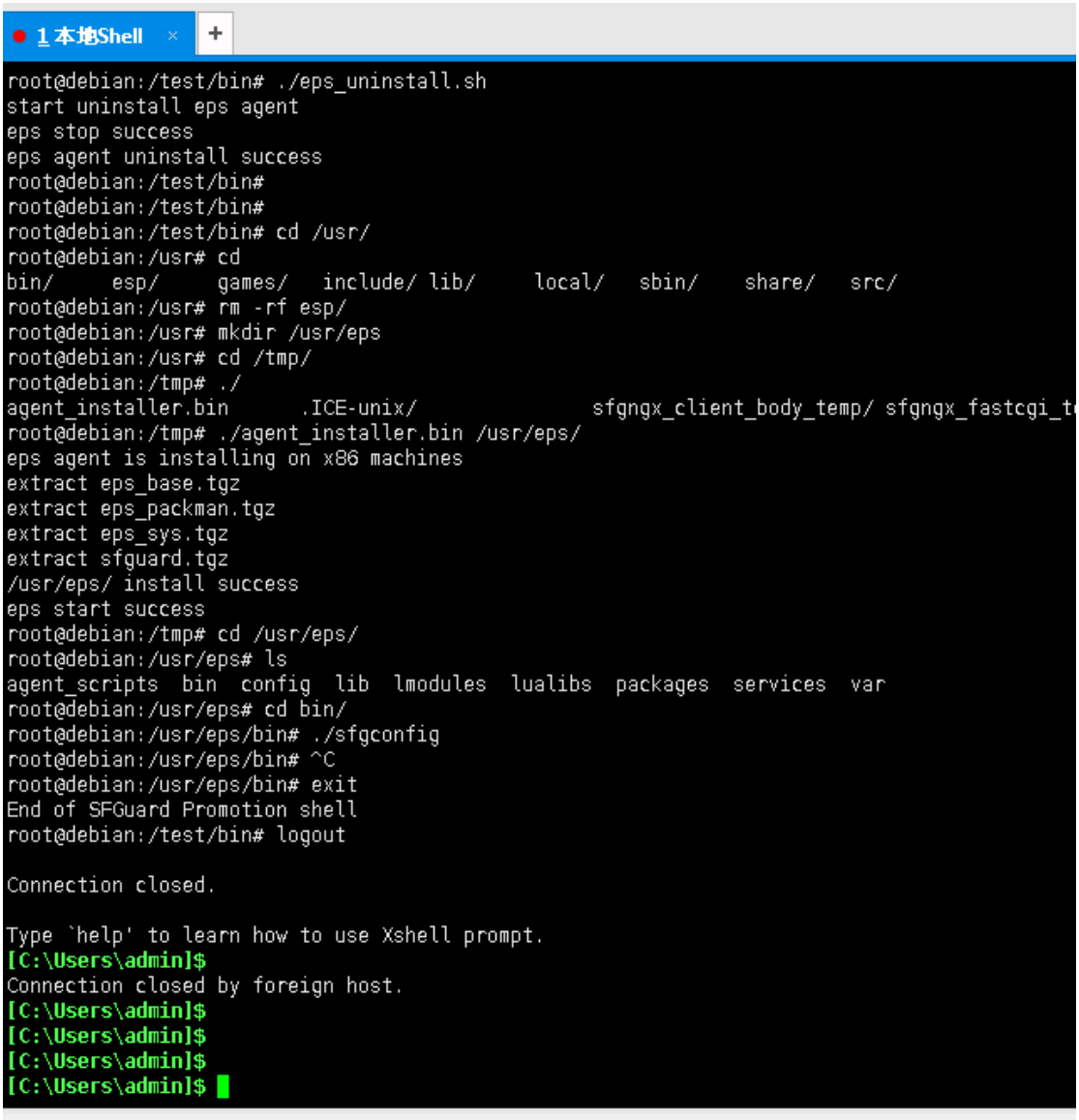
网关地址

策略名称


1 172.172.3.100:22
SFGuard config
|--- php-fpm
|--- mysqld
|--- java
|--- oracle
|==> db2sysc
Add to excluded processes: [_____]
*** Normally, SFGuard detect processes need to be protect automatically
*** You can add manually In case of detection failure
+ Included processes
Add to Included processes: [_____]
Privileged users
*** Connection from Trusted addresses are treated as previleged user
+ Trusted remote addresses
|==> 127.0.0.1
Add to address list: [_____]
Privileged HTTP Port
[X] Enable Privileged HTTP Port
Http server port: [80
Privileged proxy Port: [444
[X] Http server use HTTPS
SSL Cert file: [/ac/sfg_nginx/conf/server.crt]
SSL Key file: [/ac/sfg_nginx/conf/server.key]
Basic User-Password auth
[X] Use Basic User-Password auth
User: [admin]
Password: [**********]
按需修改http端口


1 172.172.3.100:22
SFGuard config
[X] Enable Privileged HTTP Port
Http server port: [80]
Privileged proxy Port: [444]
[X] Http server use HTTPS
SSL Cert file: [/ac/sfg_nginx/conf/server.crt]
SSL Key file: [/ac/sfg_nginx/conf/server.key]
Basic User-Password auth
[X] Use Basic User-Password auth
User: [admin]
Password: [**********]
Normal users
Replace uid while EXEC, With uid: [0]
Protected list
[X] Normal user has NO write permission in PROTECTED LIST paths
+ PROTECTED LIST(Read only)
|--- /data/www
|==> /etc/sfguard.conf
|--- /var/www
Add to PROTECTED LIST: [
+ EXCLUDE PROTECTED LIST(permitted to write)
|==> /data/www/upload
Add to EXCLUDE PROTECTED LIST: [
[Save]
[Quit]

保存退出

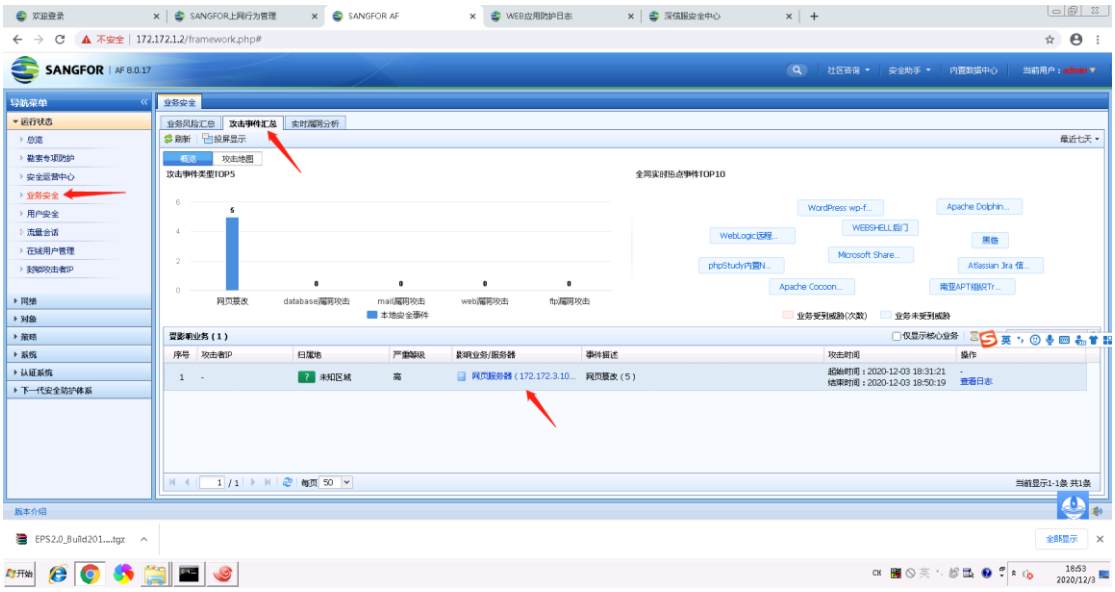


四、 验证:

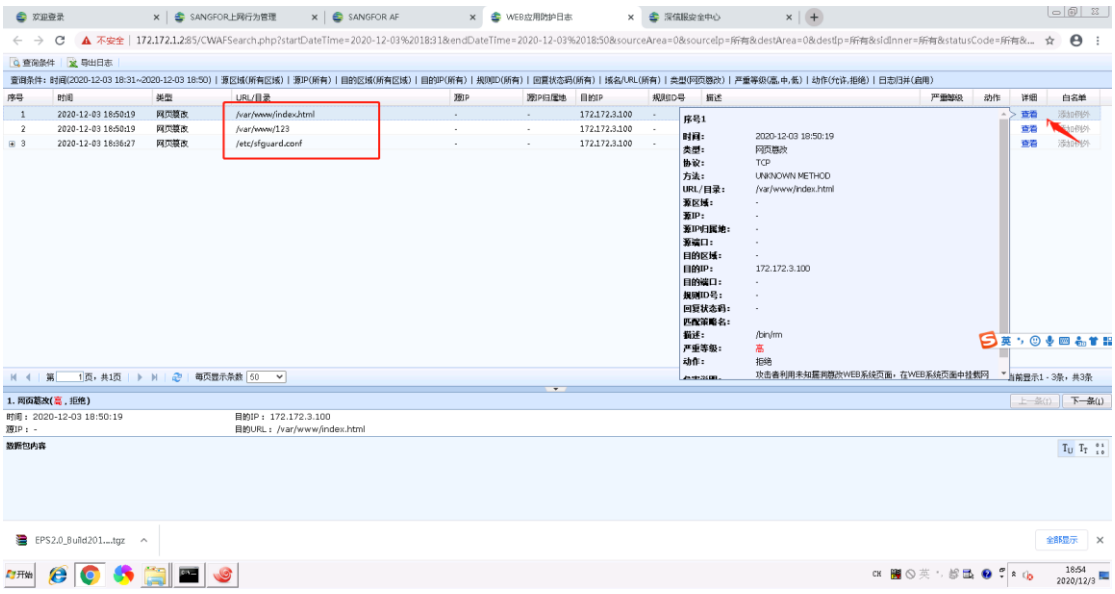
1、测试服务器端是否可以写入、删除文件

```
[C:\Users\admin]$
[C:\Users\admin]$ ssh root@172.172.3.100


Connecting to 172.172.3.100:22...
Connection established.
To escape to local shell, press 'Ctrl+Alt+]'.

Linux debian 2.6.32-5-686 #1 SMP Mon Jan 16 16:04:25 UTC 2012 i686

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Thu Dec  3 18:24:12 2020 from 172.172.4.10
root@debian:~# cd /var/www/
root@debian:/var/www# ls
DVWA  index.html  jcsweb  tools  wordpress
root@debian:/var/www# mkdir 123
mkdir: 无法创建目录"123": 权限不够
root@debian:/var/www# rm -rf index.html
rm: 无法删除"index.html": 权限不够
root@debian:/var/www#
```

2、登录 AF2，查看是否有获取到日志



点击查看日志，查看日志详情



3、登录后台，查看是否会跳出邮件认证