

# 堡塔云WAF安 装使用教程

□ǒ□□□



# 目 录

## 堡塔云WAF单机版

产品简介

工作原理

演示站(Demo)

安装堡塔云WAF

添加防护网站

    接入堡塔云WAF(未使用CDN)教程

    使用CDN时，如何接入堡塔云WAF

常用设置

更新堡塔云WAF

常见问题

    今日请求数、今日访问为0，如何解决？

    301重定向的次数过多

    如何迁移到新的服务器

    动态口令认证-二步认证

常用命令

更新日志

## 堡塔云WAF集群版

产品简介

工作原理

安装主控

添加防护网站

安装被控

更新日志

## 恶意IP共享计划

# 堡塔云WAF单机版

---

## 堡塔云WAF单机版本

- [产品简介](#)
- [工作原理](#)
- [演示站\(Demo\)](#)
- [安装堡塔云WAF](#)
- [添加防护网站](#)
  - [接入堡塔云WAF\(未使用CDN\)教程](#)
  - [使用CDN时，如何接入堡塔云WAF](#)
- [常用设置](#)
- [更新堡塔云WAF](#)
- [常见问题](#)
  - [今日请求数、今日访问为0，如何解决？](#)
  - [301重定向的次数过多](#)
  - [如何迁移到新的服务器](#)
  - [动态口令认证-二步认证](#)
- [常用命令](#)
- [更新日志](#)
- [恶意IP共享计划](#)

# 产品简介



## 堡塔云WAF

btwaf BTWAF openresty luajit release v3.1 Stars 28

### 堡塔云WAF

免费的私有云WAF防火墙

堡塔云WAF经过千万级用户认证，为您的业务保驾护航，免费私有云WAF防火墙，有效拦截sql注入、xss、一句话木马、防采集等常见渗透攻击，为您的业务网站保驾护航。

## 演示站(Demo)

<https://btwaf-demo.bt.cn:8379/c0edce7a>

## 立即安装

推荐使用此安装方式

使用SSH工具登录服务器，执行以下命令安装：

- 注意需要ROOT权限执行命令

复制粘贴命令后，按回车执行命令安装

```
URL=https://download.bt.cn/cloudwaf/scripts/install_cloudwaf.sh && if [ -f /usr/bin/curl ];then curl -sSO "$URL" ;else wget -O install_cloudwaf.sh "$URL";fi;bash install_cloudwaf.sh
```

[点击查看：堡塔云WAF系统兼容表](#)



## 加入微信讨论群

---



# 工作原理

## 堡塔云WAF工作原理

堡塔云WAF是由三个主要组件构成：

- cloudwaf\_nginx（简称为nginx）用于检查和过滤恶意流量，并将流量转发给网站服务器。
- cloudwaf\_mysql（简称为mysql）用于存储攻击事件日志。
- CloudWaf 是堡塔云WAF的管理程序，提供管理界面供用户使用（简称为管理程序）。

它如何工作的？

堡塔云WAF以反向代理的方式工作。网站流量先抵达堡塔云WAF，经过堡塔云WAF检测和过滤后，再转给原来提供服务的网站服务器。

示例

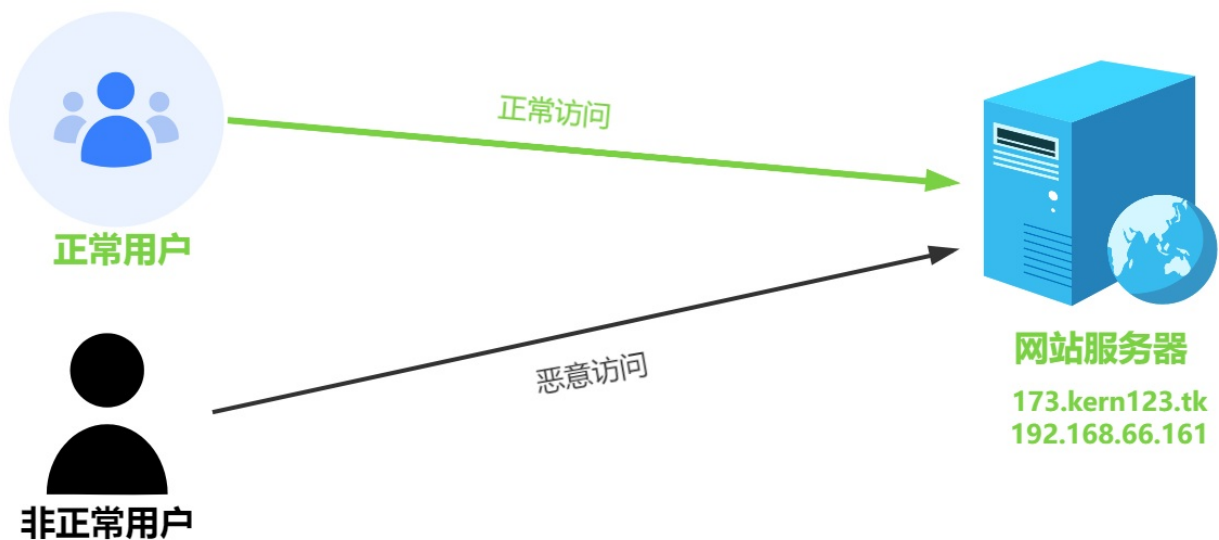
通过一个简单的例子描述如何搭建堡塔云WAF

未接入堡塔云WAF前

所有用户的流量直接流向提供网站的服务器

- 网站域名：[173.kern123.tk](http://173.kern123.tk)
- 网站服务器IP、网站域名A记录IP：192.168.66.161

如图：

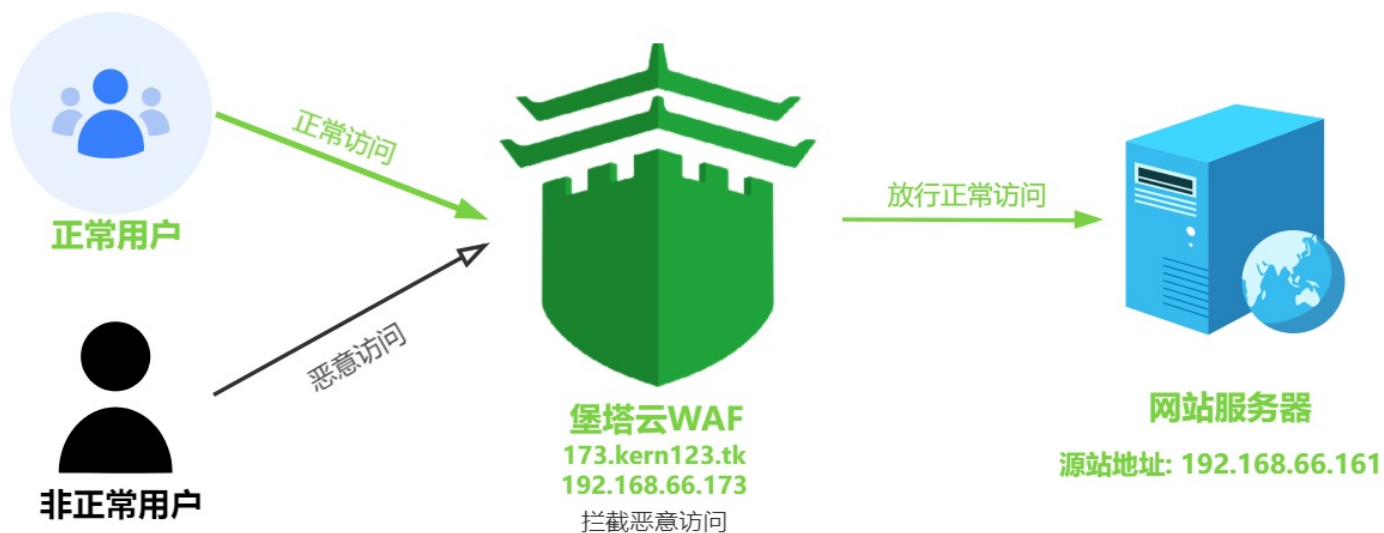


接入堡塔云WAF后

所有用户的流量先流向堡塔云WAF通过WAF过滤恶意流量后再将正常流量发送到源站服务器（网站服务器在这也称回源服务器，简称：源站地址）。

- 防护网站（网站域名）：[173.kern123.tk](http://173.kern123.tk)
- 堡塔云WAF、防护网站A记录IP：192.168.66.173
- 网站服务器IP（源站地址）：192.168.66.161

如图：



# 演示站(Demo)

---

## 演示站(Demo)

---

<https://btwaf-demo.bt.cn:8379/c0edce7a>

## 立即安装

---

推荐使用此安装方式

使用SSH工具登录服务器，执行以下命令安装：

- 注意需要ROOT权限执行命令

复制粘贴命令后，按回车执行命令安装

```
URL=https://download.bt.cn/cloudwaf/scripts/install_cloudwaf.sh && if [ -f /usr/bin/curl ];then curl -sSO "$URL" ;else wget -O install_cloudwaf.sh "$URL";fi;bash install_cloudwaf.sh
```

[点击查看：堡塔云WAF系统兼容表](#)

# 安装堡塔云WAF

## 安装方式

[点击查看：堡塔云WAF系统兼容表](#)

温馨提示：中国内地（大陆）服务器需要备案，建议您在已经备案的服务商上购买新的服务器，否则需要重新接入备案。

可参考阿里云：[接入备案流程](#)

### 在线安装

推荐使用此安装方式

使用SSH工具登录服务器，执行以下命令安装：

- 注意需要ROOT权限执行命令

复制粘贴命令后，按回车执行命令安装

```
URL=https://download.bt.cn/cloudwaf/scripts/install_cloudwaf.sh && if [ -f /usr/bin/curl ];then curl -sSO "$URL" ;else wget -O install_cloudwaf.sh "$URL";fi;bash install_cloudwaf.sh
```

```
root@wafdebian12:~#  
root@wafdebian12:~# URL=https://download.bt.cn/cloudwaf/scripts/install_cloudwaf.sh && if [ -f /usr/bin/curl ];then curl -sSO "$URL" ;else wget -O install_cloudwaf.sh "$URL";fi;bash install_cloudwaf.sh
```

安装完成后显示以下信息

```

root          hard    nofile      1000001
root          soft    nofile      1000001
正在解压文件中,请稍等...
正在安装镜像中,请稍等...
Loaded image: btwaf-openresty:latest
Loaded image: btwaf-mysql:latest
正在创建 cloudwaf_mysql 容器...
b6498cd2f09ebb6a1cec33dc7761628fce77db3b1bb2bb2abcb25cdd58be1601
正在创建 cloudwaf_nginx 容器...
a3c0cb46c30d904f755105b725059b9f05444d142e589e672a00a985b64b06b3
正在初始化堡塔云WAF...
default_user: 72377fab
default_password: d397711b
正在导入数据中
正在导入数据中,请耐心等待...
Restarting cloudwaf_nginx... done
Stopping ipfilter... done
Starting ipfilter... done
Stopping bt-cloudwaf... done
Starting bt-cloudwaf... done
Synchronizing state of btw.service with SysV service script with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable btw
Command may disrupt existing ssh connections. Proceed with operation (y|n)? Firewall is active and enabled on system startup
Default incoming policy changed to 'deny'
(be sure to update your rules accordingly)
Firewall reloaded
=====
堡塔云WAF安装完成! Installed successfully!
=====
外网访问地址: https://[redacted]:8379/a01907f7
内网访问地址: https://192.168.66.173:8379/a01907f7
username: 72377fab
password: d397711b
If you cannot access the Bt-WAF
release the following Bt-WAF port [8379] in the security group
若无法访问堡塔云WAF, 请检查防火墙/安全组是否有放行[8379]端口
=====打开堡塔云WAF前请看=====
默认启用自签证书https加密访问, 浏览器将提示不安全
点击【高级】-【继续访问】或【接受风险并继续】访问
参考教程: https://www.bt.cn/bbs/thread-117246-1-1.html
=====
Time consumed: 1 Minute!
root@cloudwaf-12: #

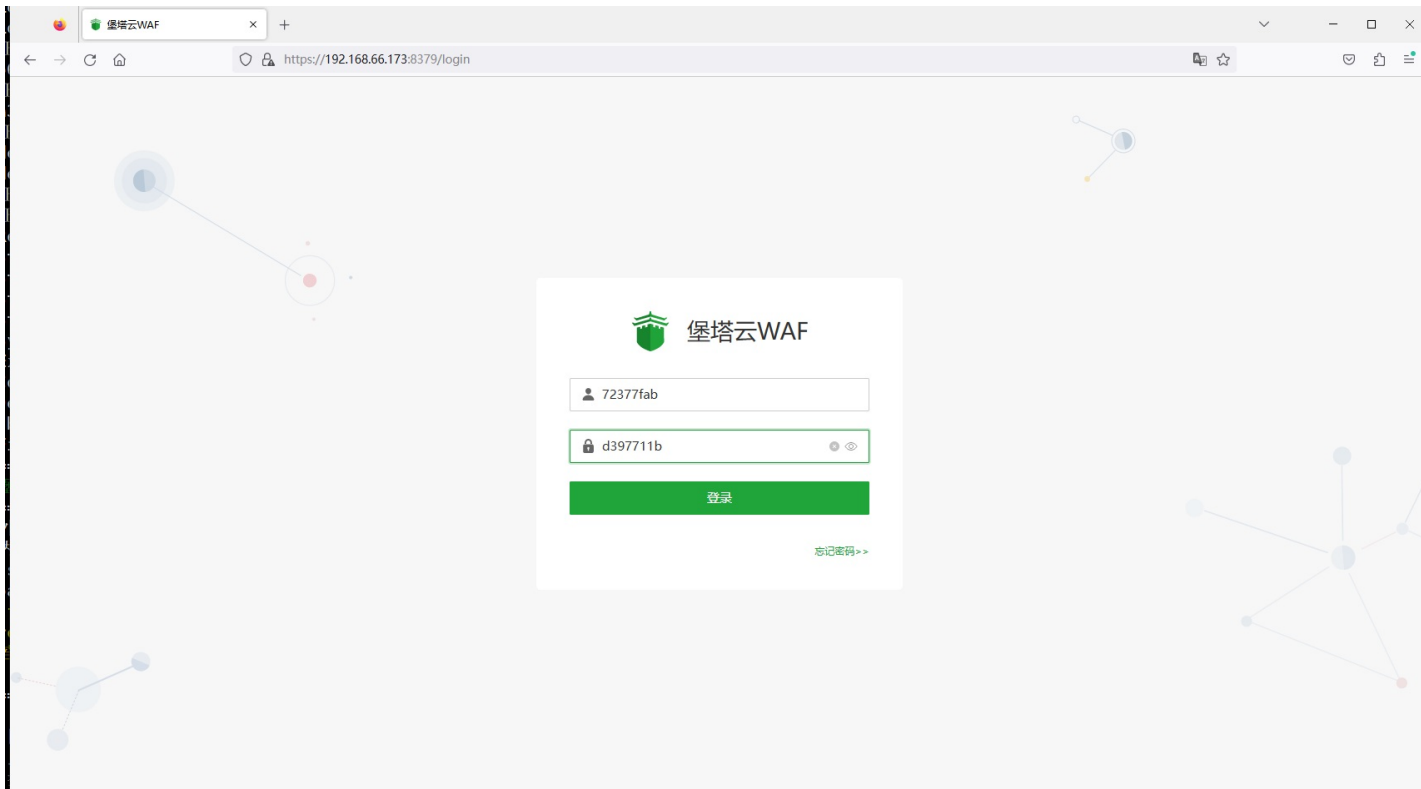
```

## 登录堡塔云WAF管理面板

管理面板默认端口8379, 如果服务器有安全组、硬件防火墙, 请开放8379端口

安装完成后, 使用浏览器访问显示的地址, 输入账号(username)与密码(password), 登录堡塔云WAF管理界面

注意: 浏览器提示安全问题, 请信任它。因为自签证书浏览器不信任导致的



## 登录成功后即可使用堡塔云WAF

今日请求数

**449552**

恶意请求数

**35**

请求趋势

网站QPS: 21/s

实时回源: 84.33ms

网站流量 发送: 95.11 KB 接收: 5.98 KB

最新慢请求

时间	URI	访问时间
09-15 16:37:09	/dj/9-aapanel-linux-panel-673-i...	10712ms
09-15 16:34:30	/dj/12356-setting-not-work-afte...	3862ms
09-15 16:34:29	/dj/9-aapanel-linux-panel-673-i...	15001ms
09-15 16:34:25	/dj/9/698?btwaf=9589174	11882ms
09-15 16:32:37	/api/discussions?filter%5Bq%5...	2039ms
09-15 16:32:21	/dj/17892-an-error-occurred-w...	3440ms
09-15 16:32:20	/dj/17888-an-error-occurred-w...	2400ms
09-15 16:31:16	/dj/9-aapanel-linux-panel-678-i...	12763ms

攻击地图 (30天)

IP攻击排行TOP10 (30天)

攻击IP	攻击次数	IP归属地
5.161.131.48	11	美国
203.175.10.230	10	印尼
119.45.252.85	9	江苏 - 南京
2a09:bac5:3b13:1028::...	7	印度
14.215.176.208	2	广东 - 广州
34.101.121.7	2	美国
42.3.62.78	2	中国香港
185.218.6.211	2	澳大利亚
203.210.16.66	2	韩国

系统: tencentos 3.1 x86\_64

运行: 8.2 天

负载: 0.04 / 0.32 / 0.33

CPU: 2 核心 (5.03%)

内存: 665 / 1722 MB (38.66%)

最新拦截事件

访问时间	状态	域名	URI	攻击IP	IP归属地	攻击类型	操作
09-15 15:41:42	已拦截	www.aapanel.com	/index.html	85.208.98.196	美国	恶意爬虫防御	详情
09-15 14:33:46	已拦截	www.aapanel.com	/www_aapanel_com.tar.gz	14.215.176.208	广东 - 广州	恶意下载防御	详情
09-15 14:10:47	已拦截	forum.aapanel.com	/api/tags/undefined?include=children%2Cchildren.parent%2Cparent%2Cst...	180.191.247.189	菲律宾	目录扫描防御	详情
09-15 14:10:47	已拦截	forum.aapanel.com	/api/tags/undefined?include=children%2Cchildren.parent%2Cparent%2Cst...	180.191.247.189	菲律宾	目录扫描防御	详情
09-15 14:10:47	已拦截	forum.aapanel.com	/api/tags/undefined?include=children%2Cchildren.parent%2Cparent%2Cst...	180.191.247.189	菲律宾	目录扫描防御	详情
09-15 14:10:47	已拦截	forum.aapanel.com	/api/tags/undefined?include=children%2Cchildren.parent%2Cparent%2Cst...	180.191.247.189	菲律宾	目录扫描防御	详情
09-15 14:10:47	已拦截	forum.aapanel.com	/api/tags/undefined?include=children%2Cchildren.parent%2Cparent%2Cst...	180.191.247.189	菲律宾	目录扫描防御	详情
09-15 14:10:47	已拦截	forum.aapanel.com	/api/tags/undefined?include=children%2Cchildren.parent%2Cparent%2Cst...	180.191.247.189	菲律宾	目录扫描防御	详情

## 离线安装

注意，此安装方式适用于服务器无法连接公网节点时的选择

- 离线安装时必须手动安装 docker，否则无法安装
- 离线安装前请确保您的服务器存在 tar gzip curl netstat ss docker 命令，可以使用此命令检查是否存在：

```
Packs=("curl" "tar" "gzip" "netstat" "ss" "docker" ); for pack in "${Packs[@]}";  
do command -v "$pack" >/dev/null 2>&1 || echo -e "\033[31mError: $pack 命令不存  
在\033[0m"; done
```

请根据您的系统架构下载安装文件，使用命令 `uname -m` 可以查看架构

x86\_64 架构：

- 离线安装脚本：[点击下载离线安装脚本](#)
- 下载镜像文件：[点击下载镜像 x86\\_64 架构文件](#)
- 下载cloudwaf程序文件：[点击下载cloudwaf程序 x86\\_64 架构文件](#)

aarch64 架构：

- 离线安装脚本：[点击下载离线安装脚本](#)
- 下载镜像 aarch64 架构文件：[点击下载镜像 aarch64 架构文件](#)
- 下载cloudwaf程序 aarch64 架构文件：[点击下载cloudwaf程序 aarch64 架构文件](#)

根据不同的系统架构下载文件后，使用Xftp、Winscp等工具上传到服务器中，将下载的文件放在相同的路径，然后执行安装命令离线安装：

注意需要ROOT权限执行命令

```
bash install_cloudwaf.sh offline
```

安装完成后，登录步骤与在线相同 示例为：x86\_64 架构



```
root@wafdebian12:~/tnt# ls -al
total 233996
drwxr-xr-x 2 root root    4096 Sep 13 05:25 .
drwx----- 4 root root    4096 Sep 13 05:25 ..
-rw-r--r-- 1 root root 198132620 Aug 31 08:58 btwaf_mysql_openresty-latest.tar.gz
-rw-r--r-- 1 root root  41391084 Sep 13 03:01 cloudwaf-latest.tar.gz
-rw-r--r-- 1 root root    69823 Sep 11 05:05 install_cloudwaf.sh
root@wafdebian12:~/tnt# bash install_cloudwaf.sh offline
```

- 安装方式

- [点击查看：堡塔云WAF系统兼容表](#)
- [在线安装](#)
- [登录堡塔云WAF管理面板](#)
- [登录成功后即可使用堡塔云WAF](#)
- [离线安装](#)
- 请根据您的系统架构下载安装文件，使用命令 `uname -m` 可以查看架构

# 添加防护网站

## 添加防护网站

网站列表 --> 添加防护网站

名词说明：

防护域名

输入您要防护的网站域名

开启SSL

开启后可以使用 `https` 方式访问网站，否则只能使用 `http`，如原来有证书需要将证书拷贝并部署到云WAF上

源站地址

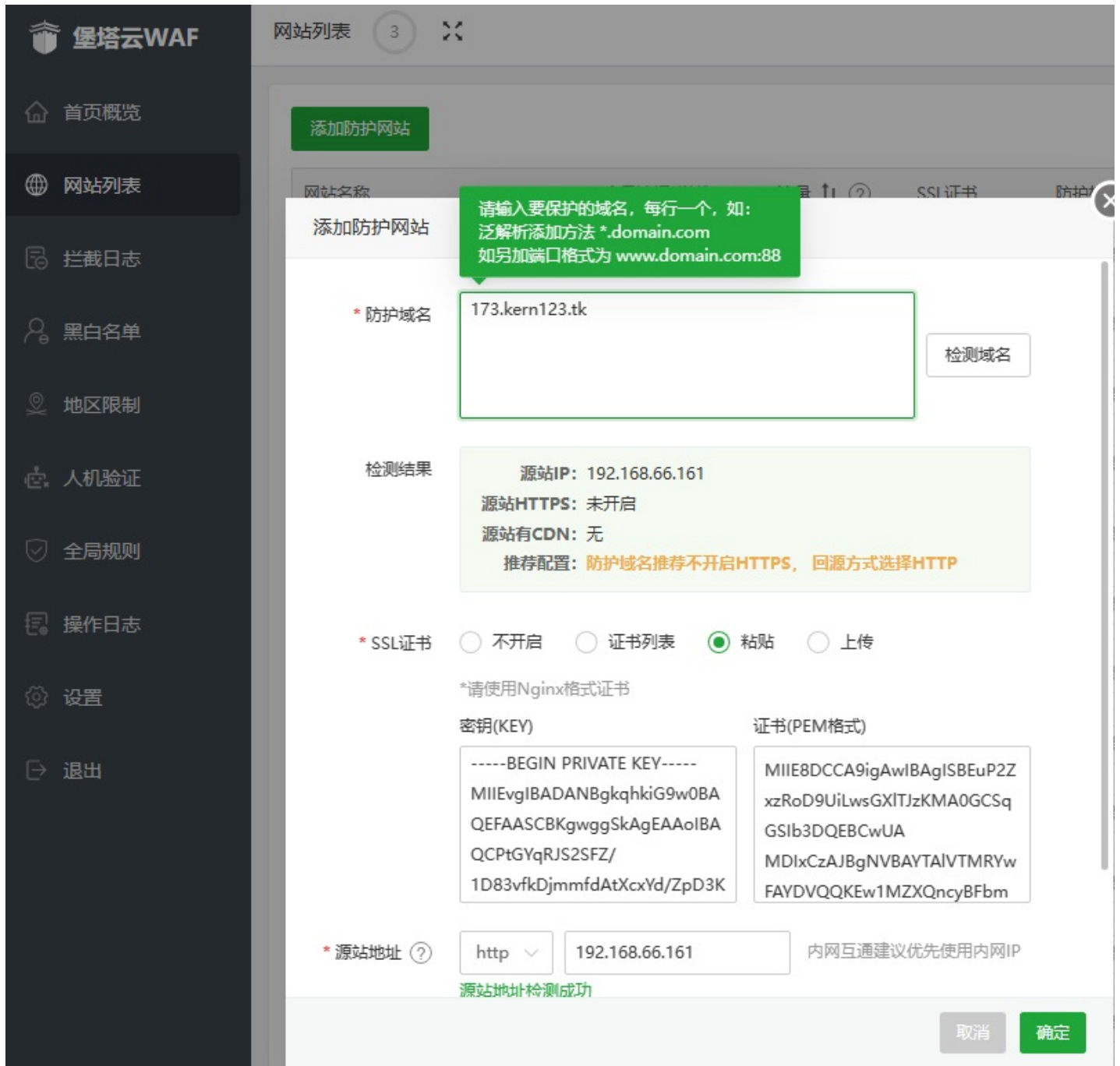
需要防护域名原来所在的服务器IP

- 如：`bt.cn`原来的IP解析在`1.2.3.4`，那么`1.2.3.4`就是它的 源站地址
- 如果原来的网站有设置SSL证书可以使用 `https`，否则请使用 `http`，设置错误浏览器将提示502错误，无法访问回源服务器
- 如果网站有使用 强制HTTPS，请使用 `https` 并且部署SSL证书，否则将提示重定向过多

CDN

堡塔云WAF前是否使用了CDN、高防或其他代理？如果不确定建议设置为开启

最后更换网站域名的A记录解析，更换为堡塔云WAF服务器的IP，等待生效后测试访问



如果开启了SSL可以使用 **https** 访问，否则只能使用 http 访问。不正确的访问方式将提示404错误

将 [173.kern123.tk](http://173.kern123.tk) 修改成您的 防护域名

https 访问方式：

<https://173.kern123.tk/?id=/etc/passwd>

http 访问方式：

<http://173.kern123.tk/?id=/etc/passwd>

如果无法访问请检查防火墙与安全组是否开放端口，默认需要开放 **80** **443** 端口

## 访问成功后

首页概览的 今日请求数、恶意请求数会增加1



如果请求数没有增加，请尝试检查：

1. 防护域名的A记录解析是否更换到堡塔云WAF的IP
2. 解析是否生效
3. 网站的日志是否有内容

## 拦截生效效果图



**请求存在威胁，已被拦截**

抱歉您的请求似乎存在威胁或带有不合法参数，  
已被管理员设置的拦截规则所阻断，请检查提交内容或联系网站管理员处理

可选：在回源服务器的网站配置只允许堡塔云WAF的IP访问，增加更强的防护，还可以防止恶意访问直接访问回源服务器

- 添加防护网站
  - 网站列表 --> 添加防护网站
    - 如果无法访问请检查防火墙与安全组是否开放端口，默认需要开放 **80** **443** 端口
  - 访问成功后
  - 拦截生效效果图

# 接入堡塔云WAF(未使用CDN)教程

- 网站未使用CDN，如何接入堡塔云WAF
  - 未接入堡塔云WAF前
    - 未接入堡塔云WAF前的网站架构:
  - 接入堡塔云WAF后
    - 接入堡塔云WAF后的网站架构:
  - 安装堡塔云WAF
  - 添加防护网站
    - 网站列表 --> 添加防护网站
      - 添加防护网站完成
    - 修改网站域名的A记录IP为 堡塔云WAF服务器的IP 请到域名厂商处修改A记录
      - 如何检查A记录是否生效：
  - 测试堡塔云WAF
    - 测试是否成功接入到堡塔云WAF
    - 浏览器直接访问网站的域名
    - 如果无法访问请检查防火墙与安全组是否开放端口，默认需要开放 **80** **443** 端口
    - 测试防护是否生效
    - 从堡塔云WAF查看访问数据
    - 教程总结

## 网站未使用CDN，如何接入堡塔云WAF

本教程略过源网站的搭建，默认您的网站已经可以正常访问后再接入云WAF。

### 未接入堡塔云WAF前

未接入堡塔云WAF前的网站架构:

用户直接访问网站服务器

如图 用户 --> 网站服务器



网站域名与解析的A记录信息：

A	156	192.168.66.152	仅 DNS - reserved IP	1 分钟	<a href="#">编辑</a>
---	-----	----------------	---------------------	------	--------------------

192.168.66.152 0

首页 网站 FTP 数据库

PHP项目 Java项目 Node项目 Go项目 Python项目 其他项目

添加站点 修改默认页 默认站点 PHP命令行版本 HTTPS防窜站 漏洞扫描

网站名

156.kern123.tk

- 网站域名: 156.kern123.tk
- 网站域名解析的IP : 192.168.66.152

## 接入堡塔云WAF后

接入堡塔云WAF后的网站架构:

用户的访问经过堡塔云WAF过滤，再转发访问给网站服务器

新增加一台服务器IP为：192.168.66.156

如图 用户 --> 堡塔云WAF --> 网站服务器



- 防护网站 与 网站服务器网站域名 : 156.kern123.tk
- 堡塔云WAF、防护网站A记录IP : 192.168.66.156
- 网站服务器IP ( 源站地址 ) : 192.168.66.152

## 安装堡塔云WAF

安装堡塔云WAF请参考：[安装堡塔云WAF](#)

在这里就略过安装了

安装完成，登录堡塔云WAF后添加防护网站

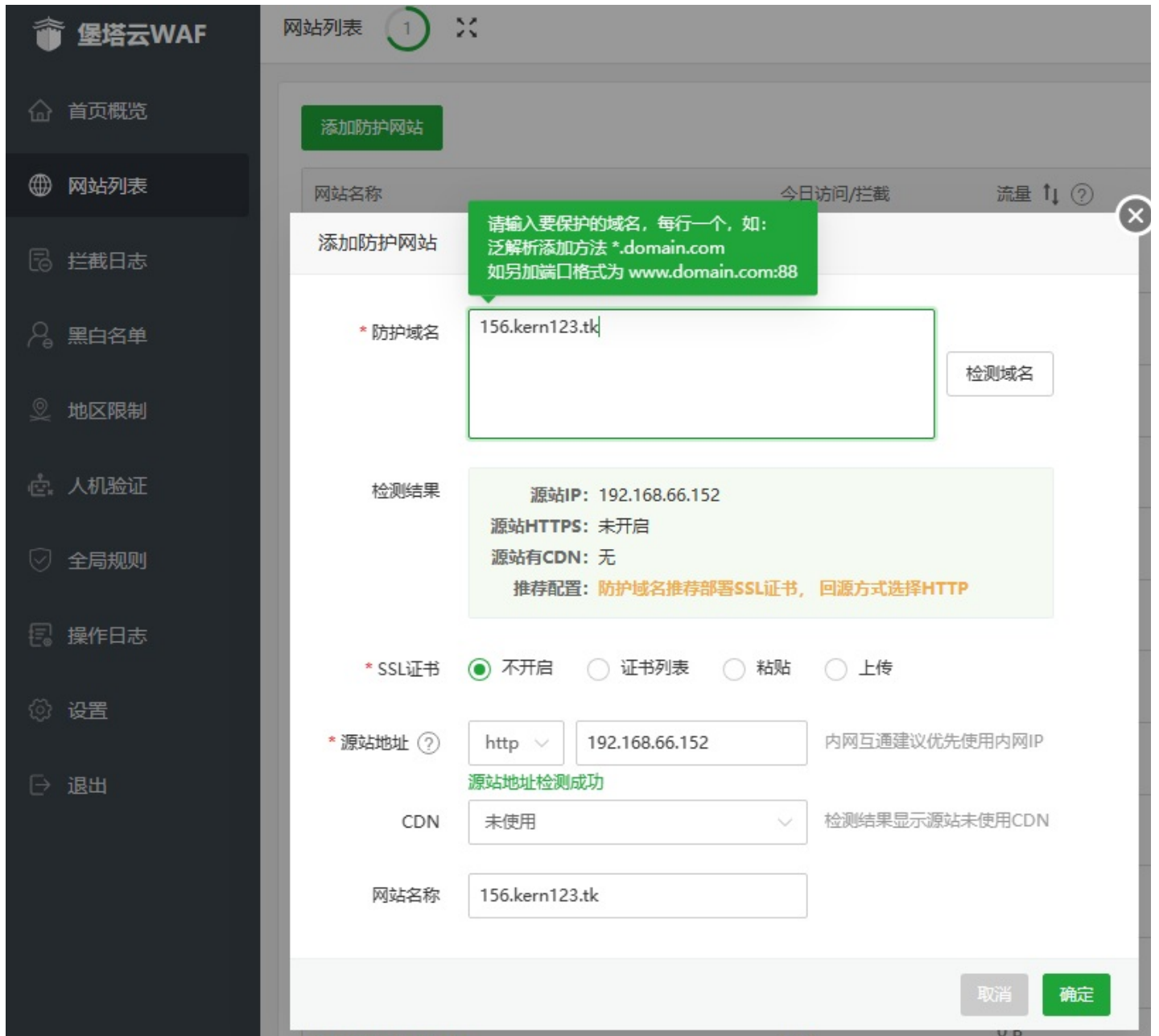
## 添加防护网站

网站列表 --> 添加防护网站

- 防护域名 : 156.kern123.tk
- 源站地址 : 192.168.66.152
  - 网站服务器的网站没有设置SSL证书，所以使用http
  - 如果设置了SSL证书可以使用 `https`
  - 如果网站有使用强制HTTPS，请使用 `https` 并且部署SSL证书，否则将提示重定向过多

提示：根据您的实际来输入，检查域名的不一定准确





## 添加防护网站完成



## 修改网站域名的A记录IP为 堡塔云WAF服务器的IP 请到域名厂商处修改A记录

从 192.168.66.152 修改成 192.168.66.156

提示：修改域名A记录需要等待1-10分钟(或更长时间)才会生效

A	156	<b>修改前的A记录</b>	192.168.66.152	←	仅 DNS - reserved IP	1 分钟	<a href="#">编辑</a>
A	156	<b>修改后的A记录</b>	192.168.66.156	←	仅 DNS - reserved IP	1 分钟	<a href="#">编辑</a>

如何检查A记录是否生效：

Windows系统可以通过 Win+R 或 点击左下角的“开始”按钮打开“开始”菜单，打开“运行”，输入 `cmd` 回车。

在命令提示符下输入 `nslookup 域名`

```
C:\WINDOWS\system32\cmd.exe
C:\Users\KERN>nslookup 156.kern123.tk
服务器: public1.114dns.com
Address: 114.114.114.114

非权威应答:
名称: 156.kern123.tk
Address: 192.168.66.152 修改前的A记录

C:\Users\KERN>
C:\Users\KERN>nslookup 156.kern123.tk
服务器: public1.114dns.com
Address: 114.114.114.114

非权威应答:
名称: 156.kern123.tk
Address: 192.168.66.156 修改后的A记录

C:\Users\KERN>
C:\Users\KERN>
```

## 测试堡塔云WAF

在域名的A记录生效后

测试是否成功接入到堡塔云WAF

- 浏览器直接访问网站的域名

使用浏览器访问网站域名：

```
http://156.kern123.tk
```

成功访问到网站：



- 服务器IP (源站IP) : 192.168.66.152

如果无法访问请检查防火墙与安全组是否开放端口，默认需要开放 **80** **443** 端口

- 测试防护是否生效

使用浏览器访问恶意链接：

```
http://156.kern123.tk/?id=/etc/passwd
```

防护生效：



请求存在威胁，已被拦截

抱歉您的请求似乎存在威胁或带有不合法参数，  
已被管理员设置的拦截规则所阻断，请检查提交内容或联系网站管理员处理

## 从堡塔云WAF查看访问数据

### 1. 首页概览

今日请求数、恶意请求数 会增加 1



### 2. 网站列表 --> [156.kern123.tk](http://156.kern123.tk)

今日访问/拦截 会增加1



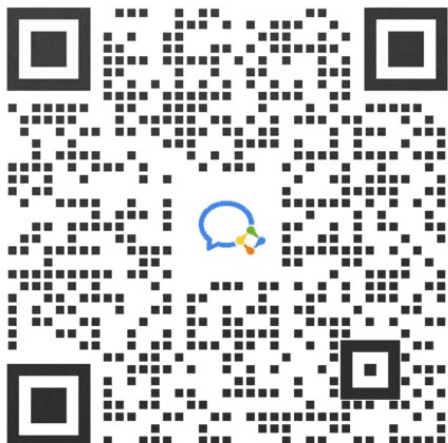
## 教程总结

- 增加：
  1. 增加服务器安装堡塔云WAF
  2. 在堡塔云WAF添加防护网站
- 修改：
  1. 修改网站域名的A记录IP
- 不变：
  1. 网站服务器配置不变
  2. 用户访问的域名不变

如果遇到问题可以参考：[常见问题](#)

如无法解决、使用中有问题，请联系我们：

加入微信讨论群



# 使用CDN时，如何接入堡塔云WAF

- 网站使用CDN时，如何接入堡塔云WAF
  - 未接入堡塔云WAF前
    - 未接入堡塔云WAF前的网站架构:
  - 接入堡塔云WAF后
    - 接入堡塔云WAF后的网站架构:
  - 安装堡塔云WAF
  - 添加防护网站
    - 网站列表 --> 添加防护网站
      - 添加防护网站完成
    - 修改CDN的回源配置IP地址为 堡塔云WAF服务器的IP，请到CDN提供商处修改回源配置
  - 测试堡塔云WAF
    - 测试是否成功接入到堡塔云WAF
    - 浏览器直接访问网站的域名
    - 如果无法访问请检查防火墙与安全组是否开放端口，默认需要开放 **80** **443** 端口
    - 测试防护是否生效
    - 从堡塔云WAF查看访问数据
    - 教程总结
  - 如果是使用 Cloudflare 如何接入？

## 网站使用CDN时，如何接入堡塔云WAF

本教程略过源网站的搭建，默认您的网站已经可以通过CDN正常访问后再接入云WAF。

本教程使用CDN的提供商为七牛云

### 未接入堡塔云WAF前

未接入堡塔云WAF前的网站架构:

用户访问CDN，CDN转发访问给网站服务器

如图 用户 --> CDN --> 网站服务器



## CDN配置与网站域名信息：

域名管理 / cdntest.kern123.tk

停用 刷新

### 基本信息

CNAME: cdntest-kern123-tk-idvmta1.qiniudns.com [复制](#) [帮助](#) 域名状态: 成功 协议: HTTP 覆盖: 海外 [修改](#)  
创建时间: 2023-09-25 15:47:59 域名类型: 普通域名 使用场景: 下载分发 IP 协议: IPv4

### 回源配置

配置项	描述	当前配置	操作
源站信息	资源的回源域名或 IP，推荐使用七牛云存储作为源站	121.40.167.103 等共 1 个	
回源 HOST	指定请求的服务器的域名，默认为加速域名。 <a href="#">帮助文档</a>	cdntest.kern123.tk	<a href="#">修改配置</a>
回源协议	请求回源的协议，如需修改回源协议请先开启 HTTPS	遵循请求协议	

首页 网站 FTP 数据库 Docker

添加站点 修改默认页 默认站点 PHP命令行版本 HTTPS防篡改 漏洞扫描

网站名	状态	备份	根目录	总流量 (切换)	到期时间	备注
cdntest.kern123.tk	运行中	无备份	/www/wwwroot/cdntest.kern123.tk	查看	永久	cdntest.kern123.tk

请选择批量操作 批量操作

- CDN域名（加速域名）、网站服务器网站域名: [cdntest.kern123.tk](#)
- CDN回源配置IP、网站服务器IP：121.40.167.103

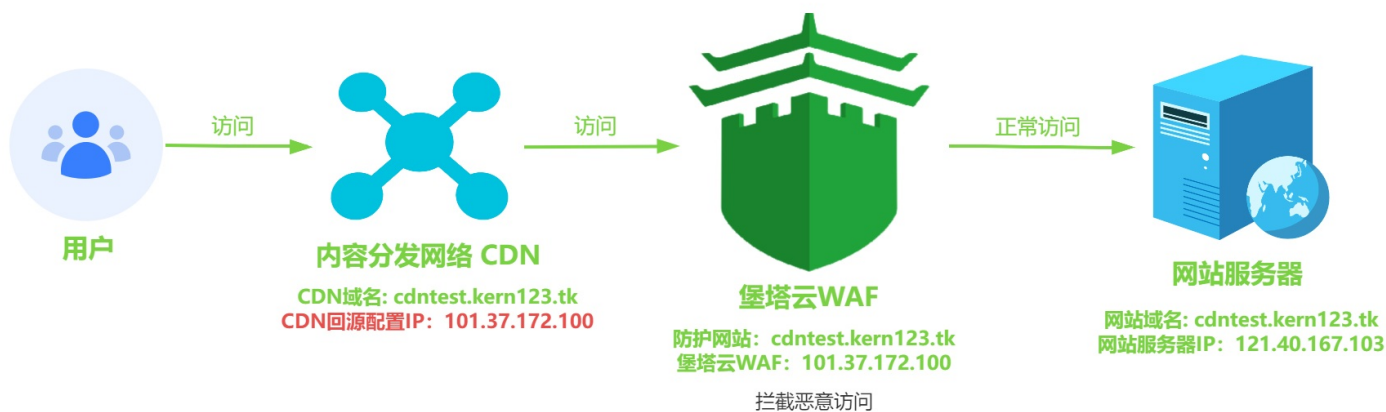
## 接入堡塔云WAF后

### 接入堡塔云WAF后的网站架构:

用户访问CDN，CDN将转发访问给堡塔云WAF过滤，再将转发访问给网站服务器

新增加一台服务器IP为：101.37.172.100

如图 用户 --> CDN --> 堡塔云WAF --> 网站服务器



- WAF防护网站、CDN域名、网站服务器网站域名：[cdntest.kern123.tk](https://cdntest.kern123.tk)
- 堡塔云WAF、CDN回源配置IP：101.37.172.100
- 网站服务器IP（源站地址）：121.40.167.103

## 安装堡塔云WAF

安装堡塔云WAF请参考：[安装堡塔云WAF](#)

在这里就略过安装了

安装完成，登录堡塔云WAF后添加防护网站

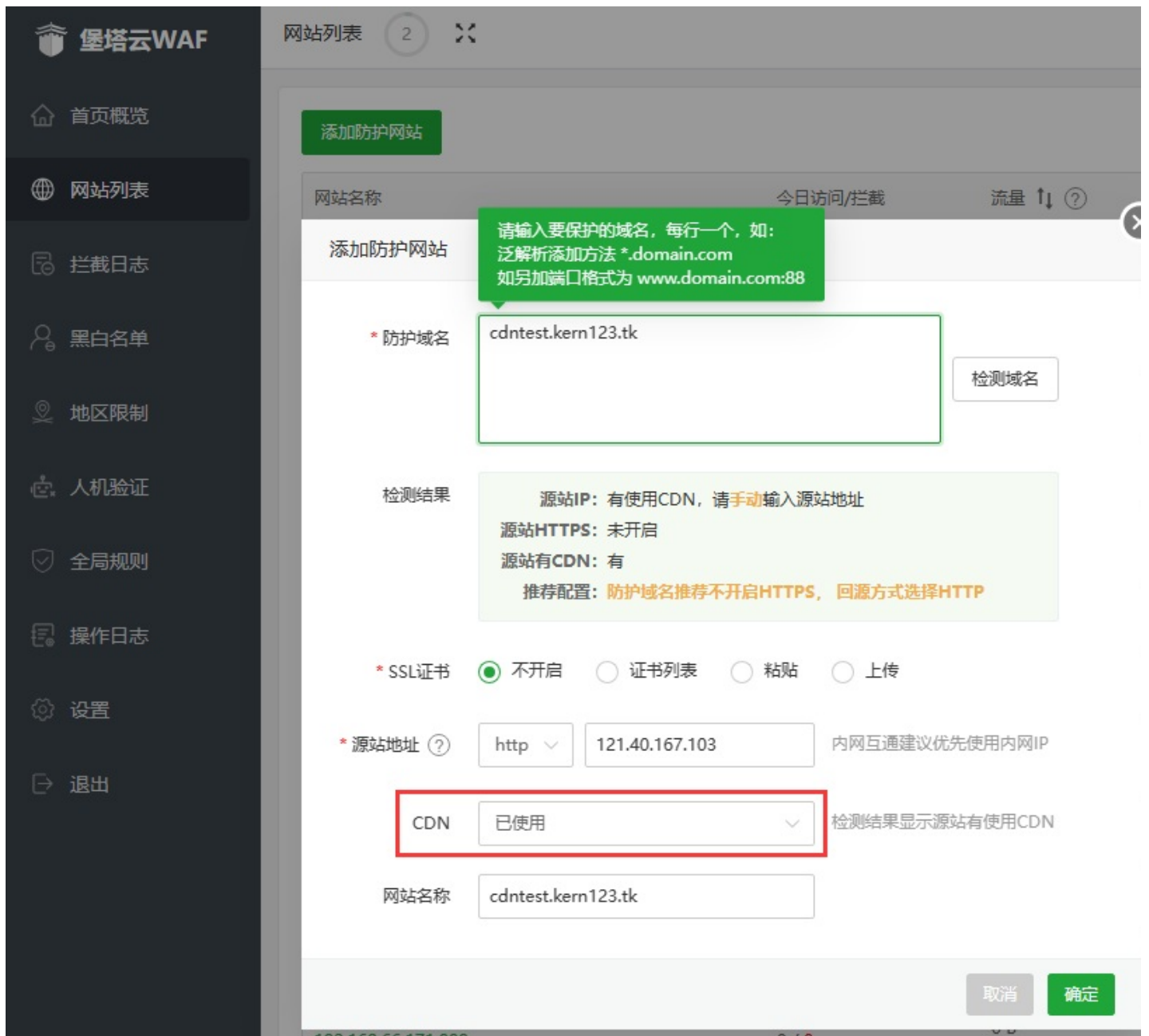
## 添加防护网站

网站列表 --> 添加防护网站

- 防护域名：[cdntest.kern123.tk](https://cdntest.kern123.tk)
- 源站地址：121.40.167.103
  - 网站服务器的网站没有设置SSL证书，所以使用http
  - 如果设置了SSL证书可以使用https
  - 如果网站有使用强制HTTPS，请使用 `https` 并且部署SSL证书，否则将提示重定向过多
- CDN：已使用
  - 请选择已使用，否则可能会拦截CDN的访问IP，导致用户无法正常访问

提示：根据您的实际来输入，检查域名的不一定准确





## 添加防护网站完成



修改CDN的回源配置IP地址为 堡塔云WAF服务器的IP，请到CDN提供商处修改回源配置

从 网站服务器IP: 121.40.167.103 修改成 堡塔云WAF的IP : 101.37.172.100

修改前：121.40.167.103

## 回源配置

X

七牛云存储  源站域名  IP 地址  高级设置

121.40.167.103

**网站服务器IP**

回源 HOST ⓘ  加速域名  自定义

去参数回源  关闭

源站测试 ⓘ

http(s)://121.40.167.1...

index.html

源站测试

资源待测试

修改后为：101.37.172.100

## 回源配置

X

七牛云存储  源站域名  IP 地址  高级设置

101.37.172.100

**堡塔云WAF的IP**

回源 HOST ⓘ  加速域名  自定义

去参数回源  关闭

源站测试 ⓘ

http(s)://101.37.172.1...

index.html

源站测试

资源待测试

源站测试通过后点击确认

注意：

本文档使用 [看云](#) 构建

请根据您的CDN回源配置修改，教程中使用的是IP地址。

如果CDN回源配置是源站域名，请将源站域名的A记录解析为堡塔云WAF的IP，并且在堡塔云WAF中添加源站域名的防护网站

提示：修改回源配置需要等待10-20分钟(或更长时间)才会生效

## 测试堡塔云WAF

在CDN提供商修改回源配置生效后

测试是否成功接入到堡塔云WAF

- 浏览器直接访问网站的域名

使用浏览器访问网站域名：

```
http://cdntest.kern123.tk
```

成功访问到网站：

```
⚠ 不安全 | cdntest.kern123.tk/index.html
```

**网站服务器IP（源站IP）：121.40.167.103**

如果无法访问请检查防火墙与安全组是否开放端口，默认需要开放 **80** **443** 端口

- 测试防护是否生效

使用浏览器访问恶意链接：

```
http://cdntest.kern123.tk/?id=/etc/passwd
```

防护生效：

```
cdntest.kern123.tk/?id=/etc/passwd
```



请求存在威胁，已被拦截

抱歉您的请求似乎存在威胁或带有不合法参数，  
已被管理员设置的拦截规则所阻断，请检查提交内容或联系网站管理员处理

## 从堡塔云WAF查看访问数据

### 1. 首页概览

今日请求数、恶意请求数 会增加 1

### 2. 网站列表 --> [cdntest.kern123.tk](http://cdntest.kern123.tk)

今日访问/拦截 会增加1

堡塔云WAF 网站列表 2

添加防护网站

网站名称	今日访问/拦截	流量 ↑↓ ?	SSL证书
cdntest.kern123.tk	1 / 1	0 B 0 B	未部署

## 教程总结

- 增加：
  1. 增加服务器安装堡塔云WAF
  2. 在堡塔云WAF添加防护网站
- 修改：
  1. 修改CDN的回源配置
- 不变：
  1. 网站服务器配置不变
  2. 用户访问的域名不变

## 如果是使用 Cloudflare 如何接入？

---

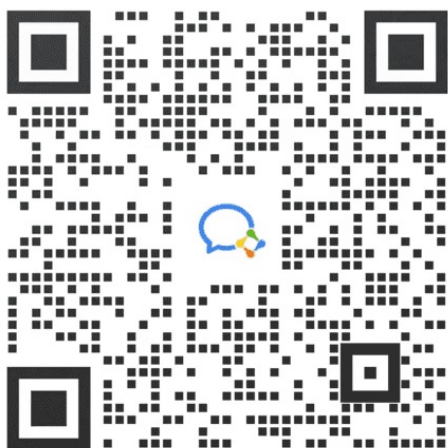
在Cloudflare管理网站中将网站域名DNS的A记录解析，修改成堡塔云WAF服务器的IP 等待生效即可。

参考：从 网站服务器IP: 121.40.167.103 修改成 堡塔云WAF的IP：101.37.172.100

如果遇到问题可以参考：[常见问题](#)

如无法解决、使用中有问题，请联系我们：

加入微信讨论群



# 常用设置

## 防护配置

- 堡塔云WAF优先级
- 为网站单独设置规则
- 查看被拦截的请求
- 查看堡塔云WAF自动拉黑IP记录
- 添加、查看手动拉黑的IP可以在：黑白名单 --> IP黑名单
- 将URL添加到URI白名单
- 如何设置只允许国内访问,同时禁止中国特别行政区:香港,澳门,台湾？
- 如何部署网站SSL证书？
  - 例：为网站156.kern123.tk部署SSL证书
- 查看网站日志

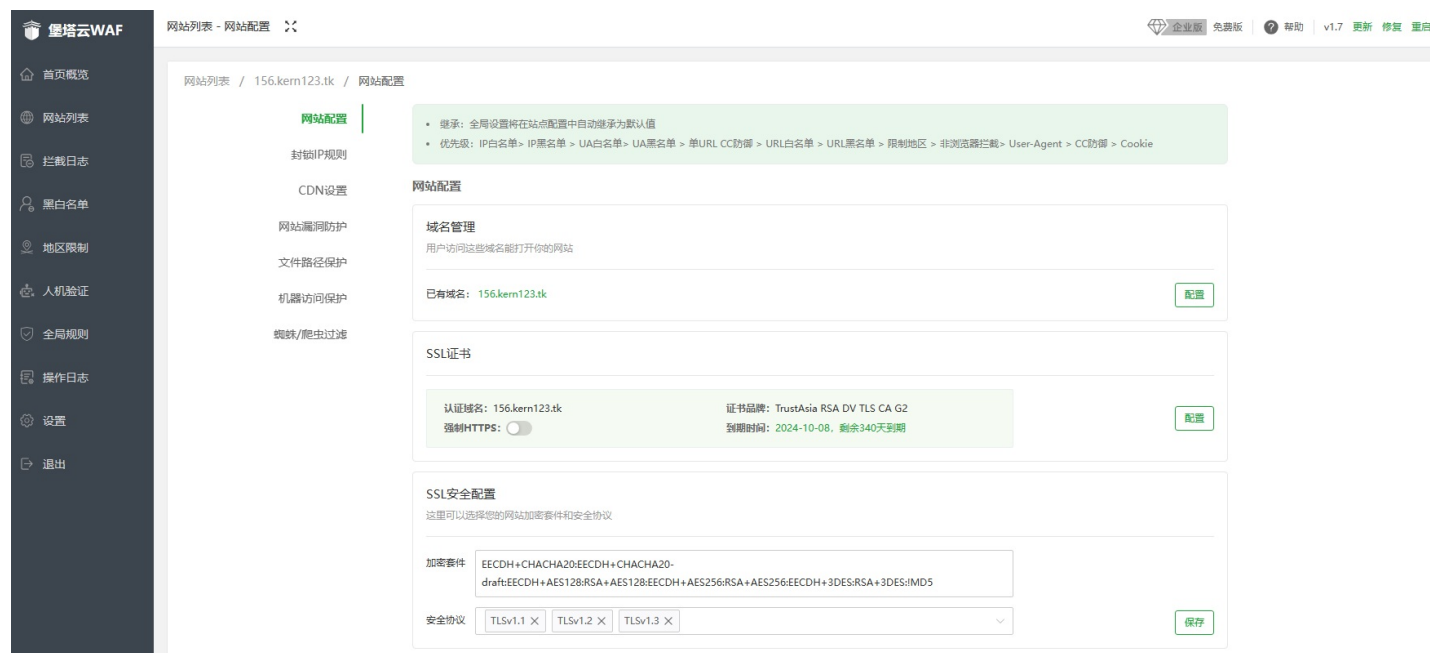
# 防护配置

## 堡塔云WAF优先级

IP白名单 > IP黑名单 > UA白名单 > UA黑名单 > 单URL CC防御 > URL白名单 > URL黑名单 > 限制地区 > 非浏览器拦截 > User-Agent > CC防御 > Cookie

## 为网站单独设置规则

网站列表 --> 找到相关网站域名 --> 网站配置



## 查看被拦截的请求

- 1. 首页概览 --> 最新拦截事件
- 2. 拦截日志 --> 拦截记录
- 3. 拦截日志 --> 规则命中记录

访问时间	状态	域名	URI	攻击IP	IP归属地	攻击类型	操作
2023-10-11 12:15:36	已拦截	192.168.66.156	/manager/radius/server_ping.php?ip=127.0.0.1[echo%20%20<?php%20echo%20md5(dlcudigjive)xunlinc(FILE_)?>>././dlcudigjive.php&id=1	192.168.1.72	内网地址	文件包含防御	拉黑 加白URL 详情
2023-10-11 12:15:36	已拦截	192.168.66.156:8011	/actuator/gateway/routes/altdsolig	192.168.1.72	内网地址	通用漏洞检测	拉黑 加白URL 详情
2023-10-11 12:15:36	已拦截	192.168.66.156:8011	/druid/indexer/v1/sampler?for=connect	192.168.1.72	内网地址	ssrf代码执行检测	拉黑 加白URL 详情
2023-10-11 12:15:35	已拦截	192.168.66.156	/manager/radius/server_ping.php?ip=127.0.0.1[cat%20/etc/passwd%20>././Test.txt&id=1	192.168.1.72	内网地址	文件包含防御	拉黑 加白URL 详情
2023-10-11 12:15:35	已拦截	192.168.66.156	/index.php?m=AjaxPersonal&a=company_focus&company_id[0]=match&company_id[1][0]=aaaaaaaa%20and%20extractvalue(1,concat(0x7e,md5(99999999)))%20-%20a	192.168.1.72	内网地址	SQL注入拦截	拉黑 加白URL 详情
2023-10-11 12:15:35	已拦截	192.168.66.156:8011	/index.php?m=AjaxPersonal&a=company_focus&company_id[0]=match&company_id[1][0]=aaaaaaaa%20and%20extractvalue(1,concat(0x7e,md5(99999999)))%20-%20a	192.168.1.72	内网地址	SQL注入拦截	拉黑 加白URL 详情
2023-10-08 15:51:27	已拦截	adminwafkern123.tk:8011	/rid=/etc/passwd	192.168.168.163	内网地址	文件包含防御	拉黑 加白URL 详情
2023-10-08 15:51:09	已拦截	adminwafkern123.tk:8011	/rid=/etc/passwd	192.168.168.163	内网地址	文件包含防御	拉黑 加白URL 详情
2023-10-08 15:51:01	已拦截	adminwafkern123.tk:8011	/index.html?id=/etc/passwd	192.168.168.163	内网地址	文件包含防御	拉黑 加白URL 详情

## 查看宝塔云WAF自动拉黑IP记录

拦截日志 --> IP临时拉黑记录

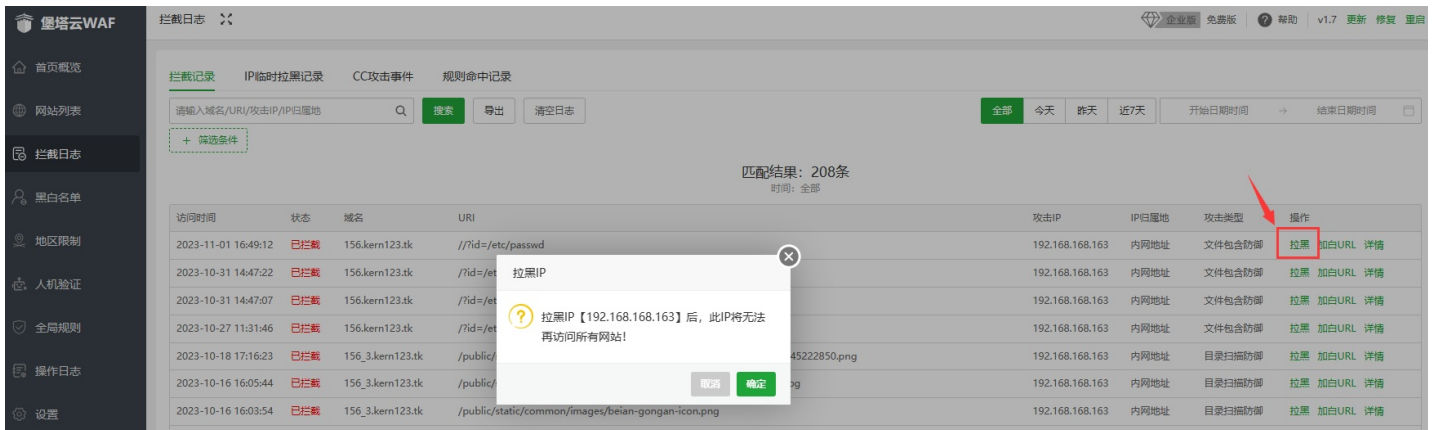
自动拉黑的IP有封锁时长，时间到达后将自动解封，解封后此IP将继续可以访问网站。如果需要永久禁止访问，请手动拉黑IP

封锁时间	状态	封锁时长	域名	URI	攻击IP	IP归属地	封锁类型	操作
2023-09-22 16:32:23	已解锁	300秒	156.kern123.tk	/index.html	192.168.66.171	内网地址	cc	解封IP 拉黑 加白URL 详情
2023-09-22 16:32:07	已解锁	300秒	156.kern123.tk	/index.html	192.168.66.171	内网地址	cc	解封IP 拉黑 加白URL 详情
2023-09-22 16:31:52	已解锁	300秒	156.kern123.tk	/index.html	192.168.66.171	内网地址	cc	解封IP 拉黑 加白URL 详情
2023-09-22 16:29:58	已解锁	600秒	156.kern123.tk	/?id=1%27union%20select%20user(1,1,3--	192.168.66.171	内网地址	多次恶意攻击	解封IP 拉黑 加白URL 详情

添加、查看手动拉黑的IP可以在：黑白名单 --> IP黑名单

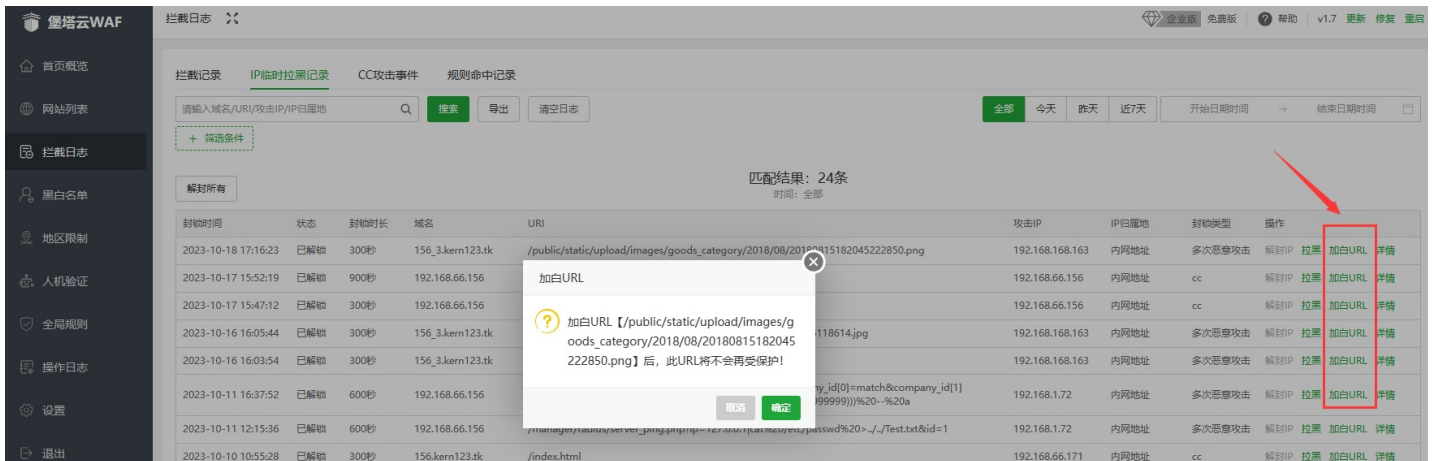
注意：拉黑的IP是会禁止访问宝塔云WAF上所有网站





## 将URL添加到URI白名单

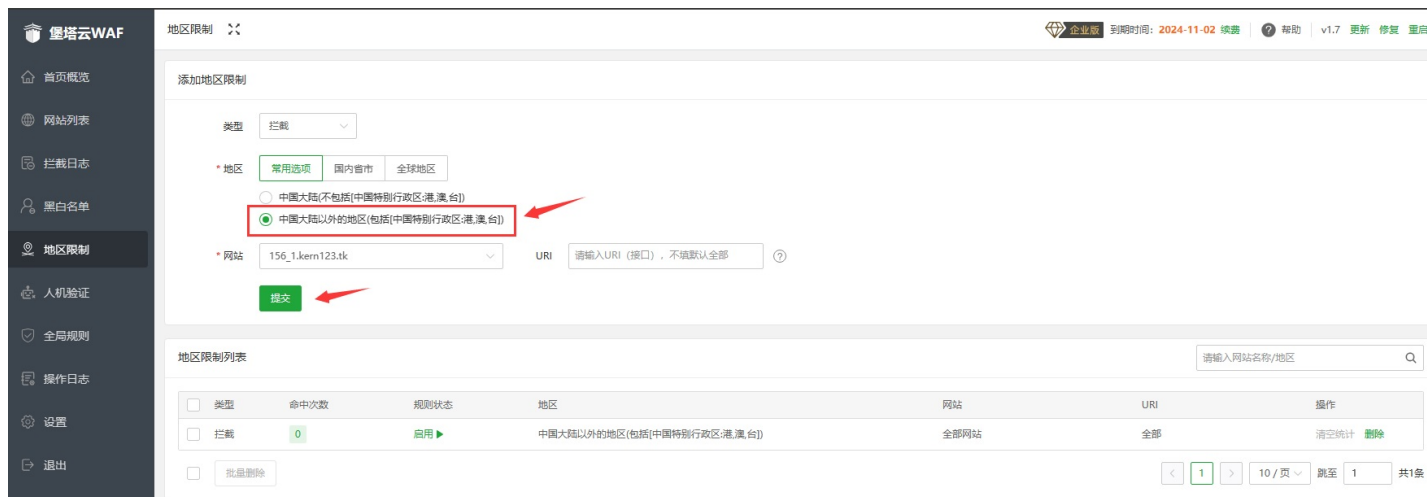
1. 黑白名单 --> URI白名单
2. 拦截日志 --> 拦截记录、IP临时拉黑记录 --> 加白URL



## 如何设置只允许国内访问,同时禁止中国特别行政区:香港,澳门,台湾 ?

地区限制 --> 添加地区限制





## 如何部署网站SSL证书?

网站列表 --> 找到您需要部署SSL的网站 --> SSL证书 --> 点击 未部署

请使用Nginx格式的证书



## 例：为网站156.kern123.tk部署SSL证书





示例中使用的SSL证书为腾讯云免费证书，下载时选择Ningx

**下载证书** 体验吐槽 & 遇到问题? [加入SSL证书交流群](#) ✕

服务器类型	操作
Tomcat (pfx格式)	<a href="#">帮助</a>   <a href="#">下载</a>
Tomcat (JKS格式)	<a href="#">帮助</a>   <a href="#">下载</a>
Apache (crt文件、key文件)	<a href="#">帮助</a>   <a href="#">下载</a>
<b>Nginx (适用大部分场景) (pem文件、crt文件、key文件)</b>	<a href="#">帮助</a>   <a href="#">下载</a>
腾讯云宝塔面板 (pem文件、crt文件、key文件)	<a href="#">帮助</a>   <a href="#">下载</a>
IIS (pfx文件)	<a href="#">帮助</a>   <a href="#">下载</a>
其他 (pem文件、crt文件、key文件)	<a href="#">帮助</a>   <a href="#">下载</a>
根证书下载 (crt文件)	<a href="#">帮助</a>   <a href="#">下载</a>

- 下载后打开156.kern123.tk\_nginx.zip文件

下载 > 156.kern123.tk\_nginx.zip > 156.kern123.tk\_nginx ▼ ↻

名称	类型	压缩大小
 156.kern123.tk.csr	CSR 文件	
 156.kern123.tk.key	KEY 文件	
 156.kern123.tk_bundle.crt	安全证书	
 156.kern123.tk_bundle.pem	PEM 文件	

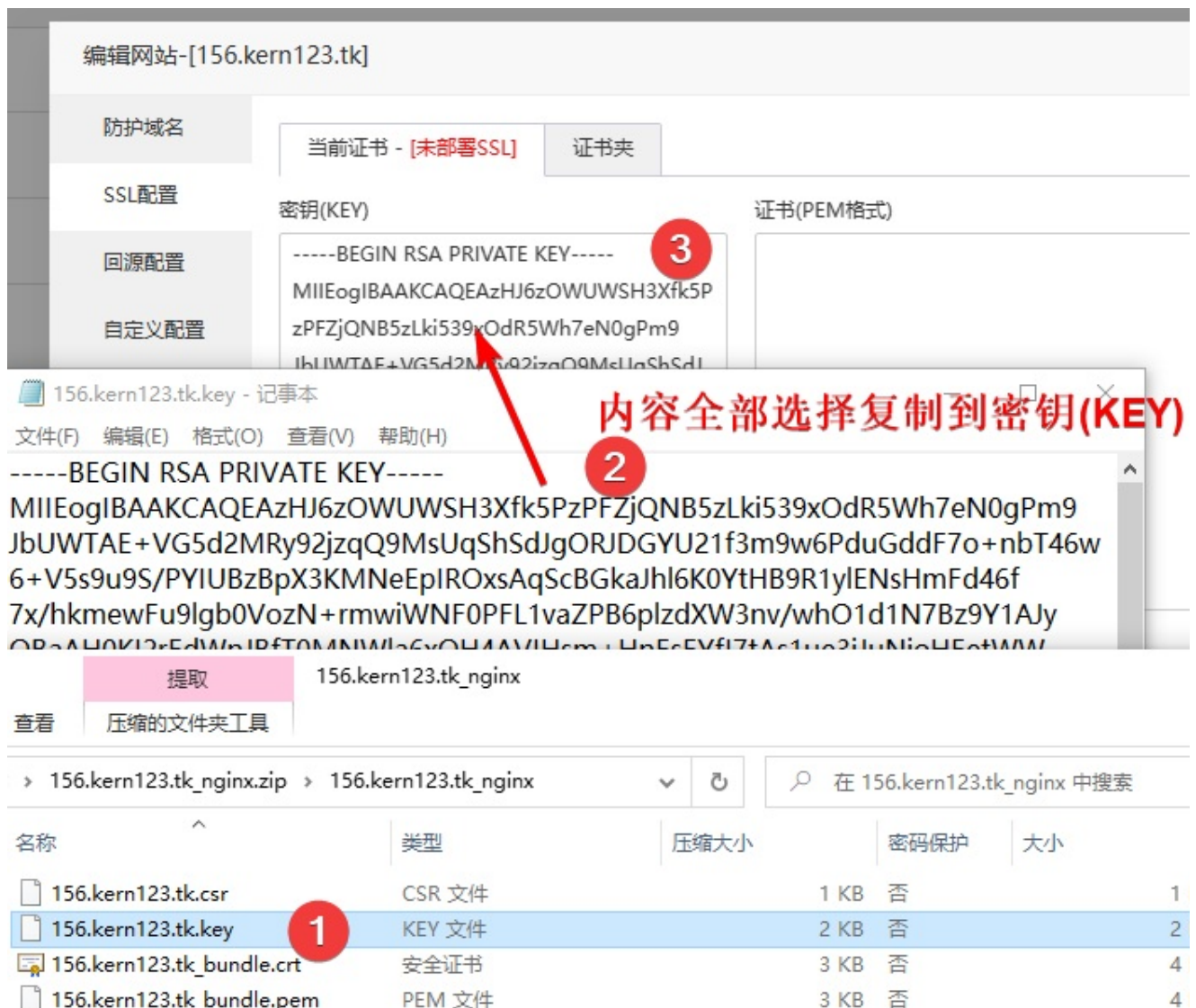
- 打开部署SSL配置界面

网站列表 --> 找到您需要部署SSL的网站 --> SSL证书 --> 点击 未部署

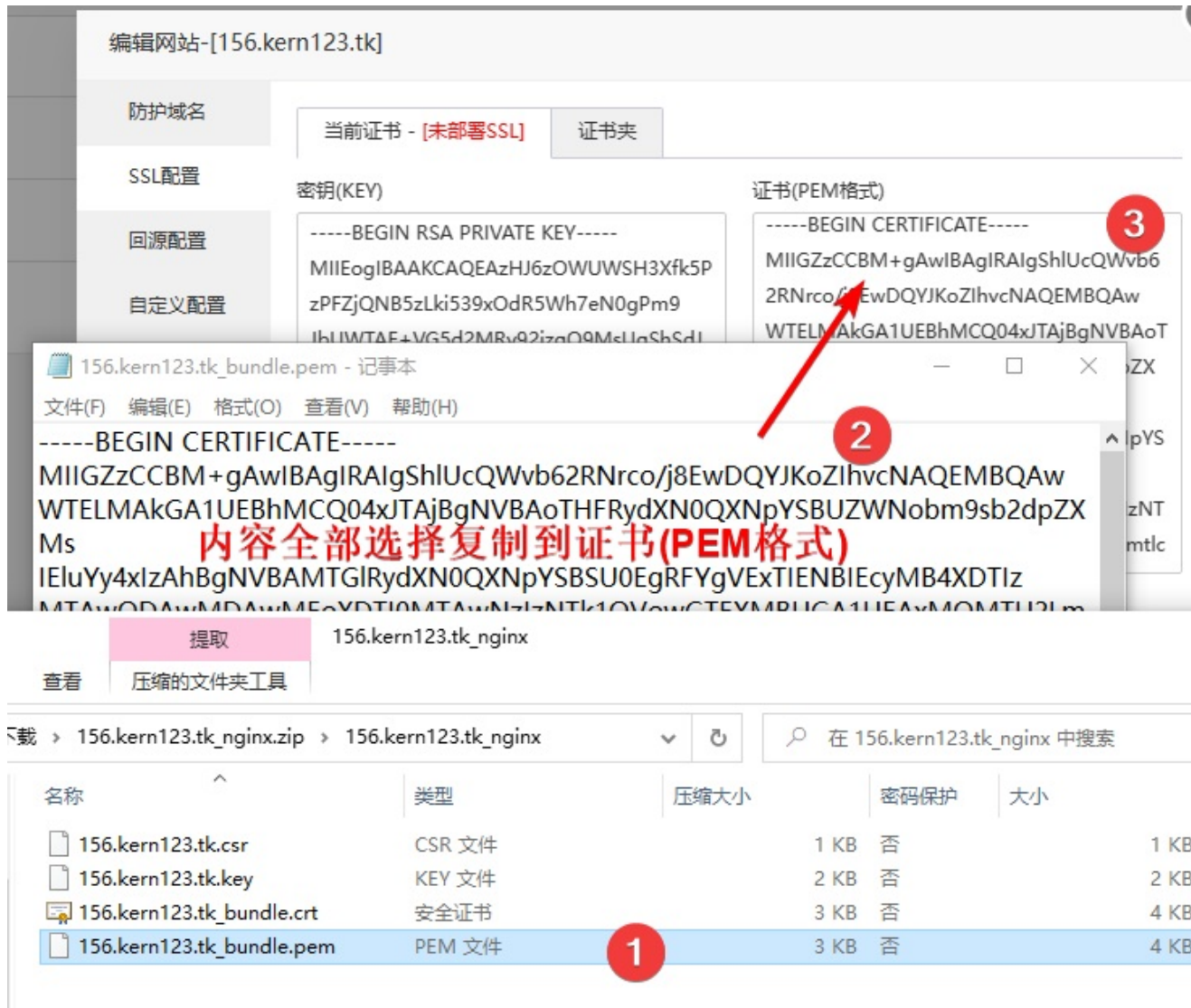


- 使用记事本 等文本编辑器打开 156.kern123.tk.key 、 156.kern123.tk\_bundle.pem

1. 将156.kern123.tk.key 的内容全部复制到 密钥(KEY) 的方框中



2. 将156.kern123.tk\_bundle.pem 的内容全部复制到 证书(PEM格式) 的方框中



- 密钥(KEY)、证书(PEM格式)粘贴完成后，点击 保存并启用 即部署完成

防护域名

SSL配置

回源配置

自定义配置

网站日志

当前证书 - [已部署SSL]
证书夹

证书品牌: TrustAsia RSA DV TLS CA G2      到期时间: 2024-10-08, 剩余365天到期

认证域名: 156.kern123.tk      强制HTTPS:

密钥(KEY)

```
-----BEGIN RSA PRIVATE KEY-----
MIIIEogIBAACAQEAzHJ6zOWUWSH3Xfk5P
zPFZjQNB5zLki539xOdR5Wh7eN0gPm9
JbUWTAfE+VG5d2MRvQ2izpO9MeLlaSbSdL
gORJDG
6+V5s9u
cBGkaJh...
```

证书(PEM格式)

```
-----BEGIN CERTIFICATE-----
MIIGZzCCBM+gAwIBAgIRAgShlUcQWvb6
2RNrco/j8EwDQYJKoZIhvcNAQEMBAw
WTELMakGA1UEBhMCQ04xJTAjBgNVBAoT
NpYSBUZWNobm9sb2dpZX
gNVBAMTGRydXN0QXNpYS
BSU0EgRFYgVExTIENBIExyMB4XDTEz
MTAwODAwMDAwMFOxMTAwNzIzNT
k1OVowGTEXMBUGA1UEAxMOMTU2Lmtrc
```

保存并启用
下载证书
关闭SSL

- 部署完成可以使用 `https` 方式访问网站 : <https://156.kern123.tk>

如果无法使用https访问，请检查系统防火墙与服务器提供商的安全组是否开放443端口

<https://156.kern123.tk>

- 服务器IP (源站IP) : 192.168.1.1

**证书查看器: 156.kern123.tk**

常规(G)    详细信息(D)

---

**颁发给**

公用名(CN)    156.kern123.tk  
 组织(O)    <不是证书的一部分>  
 组织单位(OU)    <不是证书的一部分>

**颁发者**

公用名(CN)    TrustAsia RSA DV TLS CA G2  
 组织(O)    TrustAsia Technologies, Inc.  
 组织单位(OU)    <不是证书的一部分>

**有效期**

## 查看网站日志

网站列表 --> 找到需要查看的网站名称 --> 日志 --> 响应日志、错误日志



# 更新堡塔云WAF

## 在线升级

推荐使用此升级方式

- 在堡塔云WAF管理界面更新

登录堡塔云WAF管理界面，如果有新版本 更新 将有小红点，点击即可更新



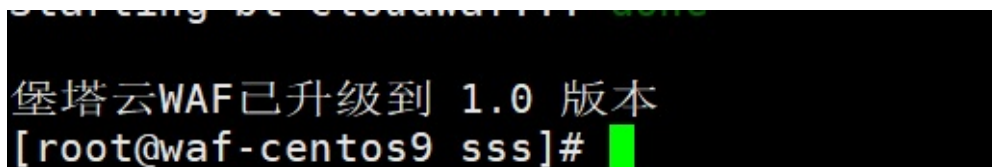
- 使用命令更新

使用SSH工具以ROOT权限登录服务器，执行以下命令进行升级：

注意需要ROOT权限执行命令，记得按回车键喔

```
btw 17
```

升级成功后会显示版本号



## 离线升级

注意，此安装方式适用于服务器无法连接公网节点时的选择

请根据您的系统架构下载安装文件，使用命令 `uname -m` 可以查看架构

x86\_64 架构：

- 升级脚本：update\_cloudwaf.sh [点击下载升级脚本](#)
- 下载cloudwaf程序 x86\_64 架构文件：[点击下载cloudwaf程序 x86\\_64 架构文件](#)

aarch64 架构：

- 升级脚本：update\_cloudwaf.sh [点击下载升级脚本](#)
- 下载cloudwaf程序 aarch64 架构文件：[点击下载cloudwaf程序 aarch64 架构文件](#)

根据不同的系统架构下载文件后，使用Xftp、Winscp等工具上传到服务器中，将下载的文件放在相同的路径，然后执行命令离线升级：

注意需要ROOT权限执行命令，记得按回车键喔。示例为：x86\_64 架构

```
bash update_cloudwaf.sh offline
```

```
[root@waf-centos9 sss]# ls -l
total 40192
-rw-r--r-- 1 root root 41115380 Sep 20 18:35 cloudwaf-latest.tar.gz
-rw-r--r-- 1 root root 40514 Sep 20 17:16 update_cloudwaf.sh
[root@waf-centos9 sss]# bash update_cloudwaf.sh offline
```

# 常见问题

- 常见问题

- 问：无法登录堡塔云WAF管理界面，如何排查？
- 问：部署堡塔云WAF后，回源服务器的网站日志全部记录为堡塔云WAF服务器的IP,如何显示真实的客户IP？
  - nginx:
- 问：网站服务器有使用Nginx防火墙、Apache防火墙等，将堡塔云WAF的服务器IP被封锁拦截了提示502。如何处理？
- 问：堡塔云WAF添加了网站，使用浏览器访问域名提示502
- 问：堡塔云WAF添加了网站，使用浏览器访问域名提示404
- 问：浏览器提示重定向次数过多 ERR\_TOO\_MANY\_REDIRECTS
- 问：堡塔云WAF是否可以与网站服务器部署在同一台服务器上
- 问：感觉增加了堡塔云WAF 后网站变慢了，如何排查？
- 问：网站一会可以访问，一会访问出错，如何排查？
- 问：发送域名如何设置？云WAF添加的网站域名与网站服务器的域名不一致如何设置
- 问：如何查看堡塔云WAF管理界面的访问链接
- 问：是否有类似bt 命令行工具
- 问：如何卸载云WAF？

## 常见问题

问：无法登录堡塔云WAF管理界面，如何排查？

答：

注意需要ROOT权限执行命令

1. 检查管理程序是否运行? 查看管理程序状态：`btw admin_status`  
如果没有启动，请尝试手动启动管理程序：`btw 2`
2. 检查是否使用完整的访问地址进行访问？查看访问地址命令：`btw 6`
3. 检查系统防火墙是否开放访问端口？
4. 服务器提供商的安全组是否开放访问端口？

问：部署堡塔云WAF后，回源服务器的网站日志全部记录为堡塔云WAF服务器的IP,如何显示真实的客户IP？



答：在回源服务器的网站配置中添加以下配置：

nginx:

```
set_real_ip_from 0.0.0.0/0 ;
real_ip_header X-Forwarded-For;
real_ip_recursive on;
```

问：网站服务器有使用Nginx防火墙、Apache防火墙等，将堡塔云WAF的服务器IP被封锁拦截了提示502。如何处理？

答：

1. 先将堡塔云WAF的服务器IP进行解除封锁
2. 在Nginx防火墙、Apache防火墙将网站的CDN开启
3. 再测试网站是否正常？

问：堡塔云WAF添加了网站，使用浏览器访问域名提示502

答：

1. 请检查源站地址配置是否正确？如果回源服务器没有开启SSL，使用 **https** 访问回源服务器将显示502错误
2. 请检查是否使用 Fail2ban防爆破、Nginx防火墙、Apache防火墙等，将云WAF的服务器IP拦截了
3. 请检查堡塔云WAF是否可以连接回源服务器（源站地址）尝试使用在堡塔云WAF服务器上执行命令检查是否可以连接：

请注意修改：“防护域名” 修改成网站域名，“源站地址” 修改成回源服务器的IP

```
curl -H "Host: 防护域名" http://源站地址
```

问：堡塔云WAF添加了网站，使用浏览器访问域名提示404

答：

1. 检查是否使用正确的访问方式？请注意区分 **https** 与 http
2. 检查回源服务器（源站地址）是否有相关域名的网站？
3. 检查在堡塔云WAF的网站域名是否正确？

## 问：浏览器提示重定向次数过多 ERR\_TOO\_MANY\_REDIRECTS

答：

1. 请检查回源服务器的网站是否设置强制HTTPS，如果有尝试关闭，浏览器使用无痕模式再访问是否正常？
2. 请检查回源服务器的网站配置是否存在错误的URL配置，其中一个URL重定向到另一个URL，而后者又重定向回前者，导致循环重定向。
3. 网站的重定向（伪静态）设置可能存在问题，导致无限循环重定向。

可以参考此教程进行排查: [301重定向的次数过多](#)

## 问：堡塔云WAF是否可以与网站服务器部署在同一台服务器上

答：

不建议这样部署，这样单服务器的负载会更高、服务器宕机概率增大。非纯净的环境会提高安装失败率。

如果能接受这些风险，堡塔云WAF也可以直接部署在网站服务器上。您需要：

将原本监听 80 或 443 端口的网站服务改到其他端口，让堡塔云WAF监听 80 或 443 端口

## 问：感觉增加了堡塔云WAF 后网站变慢了，如何排查？

答：

1. 先确认堡塔云WAF服务器与回源服务器负载是否正常？可以使用top命令检查
2. 在堡塔云WAF服务器执行命令，检查堡塔云WAF服务器与回源服务器的网络：

请注意修改：“防护域名” 修改成网站域名，“源站地址” 修改成回源服务器的IP

```
Site="防护域名"  
Source="源站地址"
```

```
curl -H "Host: ${Site} " -v -o /dev/null -s -w ' 总请求时间: %{time_total}\n HTTP  
P响应状态码: %{http_code}\n DNS解析时间: %{time_namelookup}\n 连接所花费的时间: %{ti  
me_connect}\n 从请求开始到接收到第一个字节之间的时间: %{time_starttransfer}\n 建立SSL/  
TLS连接所花费的时间: %{time_appconnect}\n' http://${Source}
```

- 如果 DNS解析时间 过大，请检查 DNS server 配置，可以尝试更换DNS
- 如果 连接所花费的时间 过大，请检查堡塔云WAF与回源服务器之间的网络状态
- 如果 从请求开始到接收到第一个字节之间的时间 过大，请检查回源服务器状态，是否出现系统负载过高

问：网站一会可以访问，一会访问出错，如何排查？

---

答：

1. 请检查网站服务器是否有使用waf，如果有，尝试将云WAF服务器的IP添加到白名单中或者开启CDN，再测试是否正常？
2. 检查云WAF到网站服务器的网络是否稳定？

问：发送域名如何设置？云WAF添加的网站域名与网站服务器的域名不一致如何设置

---

答：一般不只需要默认设置即可，如果云WAF添加的网站域名与网站服务器的域名不一致时使用 如：

- 云WAF上的域名是：[user.admin.com](https://user.admin.com)
- 网站服务器的域名是：[admin.admin.com](https://admin.admin.com)
- 那么 发送域名 设置为：[admin.admin.com](https://admin.admin.com)

问：如何查看堡塔云WAF管理界面的访问链接

---

答：使用SSH工具执行命令：`btw 6` 可以查看访问链接

访问地址说明：

如：<https://192.168.66.173:8379/a01907f7>

- 协议：`https`
- IP地址：`192.168.66.173`
- 端口：`8379`
- 安全入口：`/a01907f7`
- `://` 是分隔 协议 和 IP地址 的标记
- `:` 是分隔 IP地址 和 端口 的标记

问：是否有类似bt 命令行工具

---

答：有的，可以使用 `btw` 打开命令行工具

问：如何卸载云WAF？

---

答：卸载命令如下

```
URL=https://download.bt.cn/cloudwaf/scripts/install_cloudwaf.sh && if [ -f /usr/bin/curl ];then curl -sSO "$URL" ;else wget -O install_cloudwaf.sh "$URL";fi;bash install_cloudwaf.sh uninstall
```

# 今日请求数、今日访问为0，如何解决？

- 接入云WAF访问后，今日请求数、今日访问为0，如何解决？
  - 一、首先确认在云WAF服务器，执行命令检查本地是否可以访问？
    - 使用浏览器访问网站，今日访问没有增加，如何检查？
    - 首先确认您的服务器网络环境，根据网络环境进行检查：
      - 网络环境是：云服务器，并且是公网IP通信的，没有使用CDN
      - 网络环境是：云WAF服务器 和 网站服务器，是内网IP通信的
      - 网络环境是：有硬件防火墙（或者路由器）云WAF服务器 与 网站服务器 都是内网服务器并且相通
      - 网络环境是：云服务器，并且是公网IP通信的，有使用CDN
    - 最后确认无误后，再使用浏览器访问，再检查是否有增加访问记录？
  - 二、在云WAF服务器中执行命令检查本地访问不正常

## 接入云WAF访问后，今日请求数、今日访问为0，如何解决？

### 一、首先确认在云WAF服务器，执行命令检查本地是否可以访问？

请注意修改：“防护域名” 修改成网站域名

```
Site="防护域名"  
curl -v -H "Host: ${Site}" http://127.0.0.1
```

如果可以正常访问，访问记录会增加1

正常访问效果：

今日请求数、今日访问为0，如何解决？

```
root@waf-debian11:~#  
root@waf-debian11:~# Site="171.kern123.tk"  
root@waf-debian11:~# curl -v -H "Host: ${Site}" http://127.0.0.1  
* Trying 127.0.0.1:80...  
* Connected to 127.0.0.1 (127.0.0.1) port 80 (#0)  
> GET / HTTP/1.1  
> Host: 171.kern123.tk  
> User-Agent: curl/7.74.0  
> Accept: */*  
>  
* Mark bundle as not supporting multiuse  
< HTTP/1.1 200 OK  
< Server: openresty  
< Date: Fri, 24 Nov 2023 02:19:13 GMT  
< Content-Type: text/html  
< Content-Length: 594  
< Connection: keep-alive  
< Last-Modified: Sat, 18 Nov 2023 09:46:59 GMT  
< ETag: "65588813-252"  
< Accept-Ranges: bytes  
< Strict-Transport-Security: max-age=31536000  
<  
<!doctype html>  
<html>  
<head>  
  <meta charset="utf-8">  
  <title>Site is created successfully! </title>  
  <style>
```

堡塔云WAF 网站列表 2

添加防护网站

网站名称	今日访问/拦截	流量 ↑↓ ?	SSL证书
cdntest.kern123.tk	1 / 1	0 B 0 B	未部署

使用浏览器访问网站，今日访问没有增加，如何检查？

1. 请务必确认在云WAF服务器上，执行命令检查本地是否可以访问？
2. 云WAF中必须添加相应的防护网站

首先确认您的服务器网络环境，根据网络环境进行检查：

- 网络环境是：云服务器，并且是公网IP通信的，没有使用CDN
- 网络环境是：云WAF服务器 和 网站服务器，是内网IP通信的

用户 --> 云WAF --> 网站服务器

1. 请先确认 云WAF服务器的IP 与 网站服务器的IP
2. 检查网站域名的A记录解析是否更换到 云WAF服务器IP？

• 例如：

- 网站服务器的IP：1.1.1.1
- 网站域名：[kk.kern123.tk](http://kk.kern123.tk)
- 网站域名的解析IP：1.1.1.1
- 云WAF服务器的IP：2.2.2.2

需要将网站域名的解析IP：**1.1.1.1** 更换为 云WAF服务器的IP：**2.2.2.2**

A	kk	1.1.1.1	仅 DNS - reserved IP	1 分钟	编辑
类型	名称 (必需)	IPv4 地址 (必需)	TTL		
A	kk	2.2.2.2	1 分钟	修改后的记录	

更换域名的A记录解析需要 1-20分钟(或更长时间)才会生效

- 网络环境是：有硬件防火墙（或者路由器）云WAF服务器 与 网站服务器 都是内网服务器并且相通

用户 --> 网络提供商 --> 硬件防火墙（路由器）--> 云WAF --> 网站服务器

1. 请先确认 云WAF服务器的IP 与 网站服务器的IP
2. 检查硬件防火墙(路由器)设置的 端口映射 (NAT地址转换) 是否是云WAF服务器的IP？
3. 确认 云WAF的网站源地址 是否是网站服务器的IP？

• 例如：

- 网站服务器的内网IP：192.168.6.11
- 云WAF服务器的内网IP：192.168.6.222

需要将硬件防火墙的端口映射 网站服务器的内网IP：**192.168.6.11** 更换为 云WAF服务器的内网IP：**192.168.6.222**

未更换参考图：

今日请求数、今日访问为0，如何解决？

原始数据包

源区域： 内网

源地址： All

目的地址：  指定IP  网络对象

转换后数据包

源地址转换为： 不转换

目的地址转换为： 指定IP

指定IP： 192.168.6.11

端口转换为： 80

更换后的设置参考图：

原始数据包

源区域： 内网

源地址： All

目的地址：  指定IP  网络对象

转换后数据包

源地址转换为： 不转换

目的地址转换为： 指定IP

指定IP： 192.168.6.222

端口转换为： 80

云WAF的网站源地址(节点地址)：找到相关网站域名-->网站配置-->回源配置-->配置

编辑节点

\* 节点地址

负载状态

\* 连接失败次数

\* 重连时间  秒

备注

- 网络环境是：云服务器，并且是公网IP通信的，有使用CDN

用户 --> CDN --> 云WAF --> 网站服务器

1. 请先确认 云WAF服务器的IP 与 网站服务器的IP
2. 在CDN 服务器提供商中查看 CDN的回源配置 是使用 源站域名 还是 IP地址
  - 如果是 源站域名 请检查域名的记录解析是否更换到 云WAF服务器的IP ？
  - 如果是 IP地址 请检查是否修改为 云WAF服务器的IP ？



今日请求数、今日访问为0，如何解决？

- 例如：这里使用CDN的回源配置是：IP地址
  - 网站服务器的IP：121.40.167.103
  - 云WAF服务器的IP：101.37.172.100

修改前：121.40.167.103

### 回源配置 X

七牛云存储     源站域名     IP 地址     高级设置

121.40.167.103

网站服务器的IP

回源 HOST ⓘ     加速域名     自定义

去参数回源     关闭

源站测试 ⓘ   

资源待测试

修改后为：101.37.172.100

## 回源配置



- 七牛云存储  源站域名  IP 地址  高级设置

101.37.172.100

**云WAF服务器的IP**

回源 HOST ⓘ  加速域名  自定义

去参数回源  关闭

源站测试 ⓘ

资源待测试

修改 CDN配置 或者 更换域名的记录解析需要 1-20分钟(或更长时间)才会生效

最后确认无误后，再使用浏览器访问，再检查是否有增加访问记录？

如果还是没有访问记录，建议再次根据网络环境进行检查

## 二、在云WAF服务器中执行命令检查本地访问不正常

- 执行命令检查程序是否运行正常？

```
btw 3
```

- 检查nginx日志是否正常？

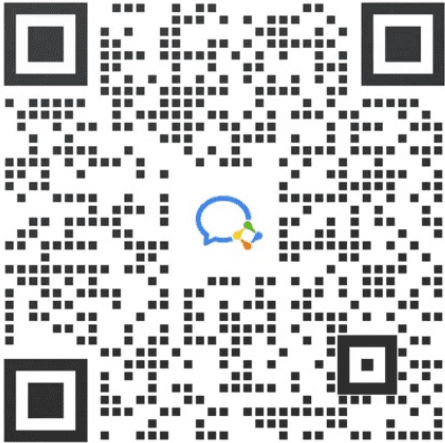
```
btw nginx_log
```

并且根据信息提示进行处理

今日请求数、今日访问为0，如何解决？

如使用中有问题，请联系我们：

加入微信讨论群



# 301重定向的次数过多

- 浏览器显示 重定向的次数过多，如何找到问题并且解决？
  - 尝试以下方法进行解决：
    - 一、首先在 网站服务器的网站 检查是否开启 强制HTTPS？
      - http 与 https 协议简单解析：
    - 二、在宝塔云WAF检查 源站IP 配置是否正确？
      - 1. 检查 源站IP 中的IP地址 确认无误是网站服务器的IP？
      - 2. 检查 源站IP 使用的协议是否正确？
      - 3. 检查 防护域名 与 网站服务器的网站域名 是否使用相同域名？
      - 4. 检查 宝塔云WAF 的防护网站是否部署SSL证书？
    - 三、最后检查配置无误后，尝试浏览器使用无痕模式再访问是否正常？如果还是重定向的次数过多，请尝试再次检查上面的配置
  - 主要检查配置：

## 浏览器显示 重定向的次数过多，如何找到问题并且解决？

重定向的次数过多

此页面不能正确地重定向

ERR\_TOO\_MANY\_REDIRECTS



### 该网页无法正常工作



将您重定向的次数过多。

尝试清除 Cookie.

ERR\_TOO\_MANY\_REDIRECTS

重新加载

此页面不能正确地重定向

连接到 : 时发生错误。

- 有时候禁用或拒绝接受 Cookie 会导致此问题。

重试

## 尝试以下方法进行解决：

### 一、首先在 网站服务器的网站 检查是否开启 强制HTTPS？

#### 强制HTTPS的配置：



- 如果只是配置了SSL证书，没有开启强制HTTPS。您可以在 堡塔云WAF的 源站IP 使用 http 或者 https
- 如果网站服务器的网站配置了 SSL证书 并且 开启了强制HTTPS。您在 堡塔云WAF的 源站IP 中的协议必须使用 **https** ，否则将出现重定向的次数过多错误

如：<https://网站服务器的IP>

#### 回源配置

设置云waf访问源站的方式

源站IP  发送域名

#### http 与 https 协议简单解析：

http 是一种用于在网络上传输超文本的协议。

http 默认使用 80 端口，使用时不需要添加端口

例：<http://171.kern123.tk>

**https** 在 http 的基础上添加了安全性，使用 SSL 或 TLS 协议对数据进行加密和身份验证 (部署SSL证书后即可使用)。

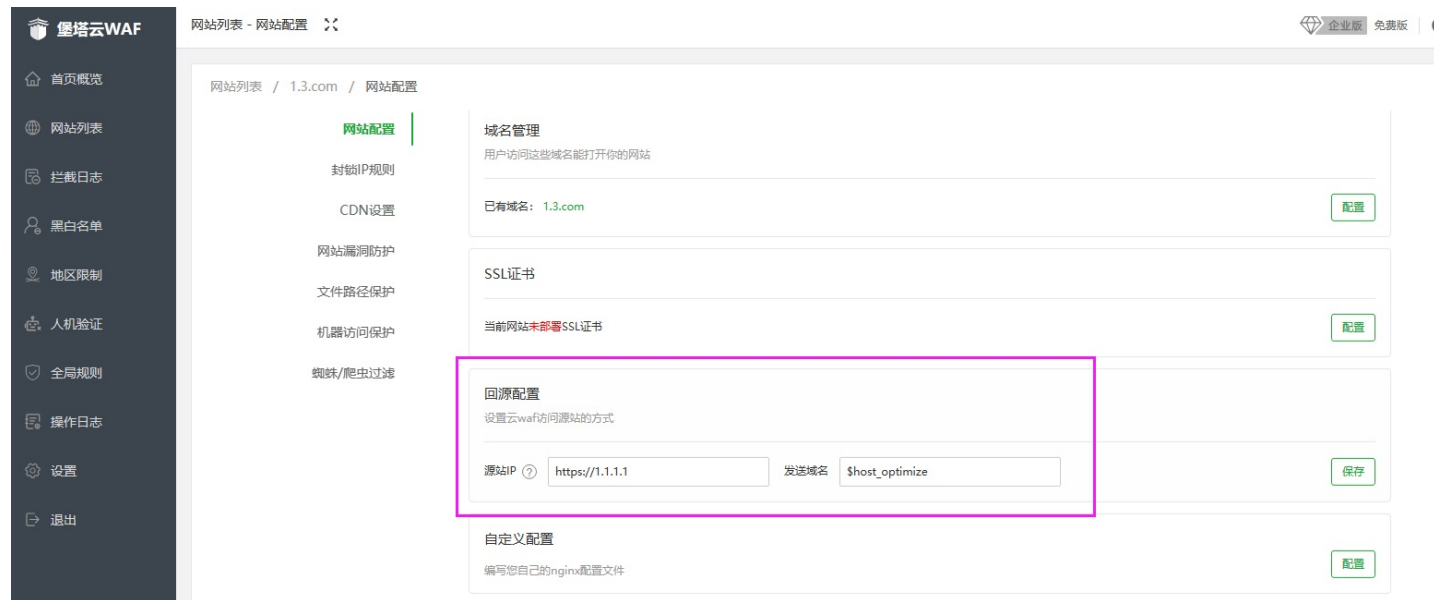
**https** 默认使用 443 端口，使用时不需要添加端口

例：<https://171.kern123.tk>注意是有s的

PS: 如果是自定义的端口需要添加

## 二、在堡塔云WAF检查 源站IP 配置是否正确？

堡塔云WAF --> 网站列表 --> 找到您的网站域名 --> 网站配置 --> 源站IP



### 1. 检查 源站IP 中的IP地址 确认无误是网站服务器的IP？

- 如果是错误的，请修改成正确的网站服务器的IP

如正确的是：<https://1.1.1.1> 错误的输入成了 <https://1.1.1.4>

- 确认无误是正确网站服务器的IP，请继续向下查看

### 2. 检查 源站IP 使用的协议是否正确？

如果只是IP地址，默认是使用 http 协议

这里的协议需要根据 网站服务器的网站配置：是否强制HTTPS 来进行决定

- 网站服务器的网站配置没有开启强制HTTPS。您可以使用 https 或者 http

- 如果网站服务器的网站配置了 SSL证书 并且 开启了强制HTTPS。您在 源站IP 中的协议必须使用 **https**  
如：<https://网站服务器的IP>

### 3. 检查 防护域名 与 网站服务器的网站域名 是否使用相同域名？

- 如果不相同请在 发送域名 输入您的 网站服务器的网站域名  
如：网站服务器的网站域名是：[a.a.com](#)，防护域名是：[b.b.com](#)  
您需要在 发送域名 中输入网站服务器的网站域名：[a.a.com](#)，然后保存。

回源配置

设置云waf访问源站的方式

源站IP ?  发送域名  保存

PS: \$host\_optimize 是使用 防护域名

### 4. 检查 堡塔云WAF 的防护网站是否部署SSL证书？

- 访问网站使用 **https** 协议，请务必部署SSL证书，否则将无法正确访问到网站。
- 源站IP 中使用的是 **https** 协议，网站服务器的网站开启了强制HTTPS，请部署SSL证书。
- 如果有使用CDN并且是使用https，请务必部署SSL证书，否则将无法正确访问到网站。

三、最后检查配置无误后，尝试浏览器使用无痕模式再访问是否正常？如果还是重定向的次数过多，请尝试再次检查上面的配置

PS：如果网站无法连接，请检查您的IP是否在 拦截日志 -- IP临时拉黑记录 中被拦截了？

### 主要检查配置：

- 网站服务器的网站 是否强制HTTPS
- 源站IP的协议是 http 还是 **https**

如无法解决、使用中有问题，请联系我们：

加入微信讨论群





# 如何迁移到新的服务器

- [如何将云WAF迁移到新的服务器?](#)
- 一、环境介绍
  - [旧的云WAF服务器环境:](#)
  - [新的服务器环境:](#)
- 二、旧的云WAF服务器需要做的步骤
  - 1. 停止WAF:
  - 2. 直接打包整个目录进行备份迁移
  - 3. 下载备份文件 `cloud_waf.tar.gz`
- 三、新的服务器需要做的步骤：
  - 1. 上传并且解压还原mysql文件
  - 2. 在新的服务器中安装云WAF
  - 3. 登录新的云WAF
  - 4. 检查云WAF功能是否正常？
  - 5. 检查网站是否正常？
- 教程总结
- [如果是同一台服务器，需要重新安装操作系统如何备份恢复？](#)
- [不同的系统架构如何迁移？](#)

## 如何将云WAF迁移到新的服务器？

迁移会影响网站的访问，建议在用户访问少时操作

堡塔云WAF版本最好是一致的

注意：检查执行的每一步是否有错误？

### 一、环境介绍

旧的云WAF服务器环境:

- 操作系统：Ubuntu 20.04
- 网站域名：[nw1.kern123.tk](#)
- 服务器IP：192.168.66.156
- 登录地址：<https://192.168.66.156:8379/5f0eb9aa>
- 云WAF帐号与密码：5c32ce9b

## 新的服务器环境:

- 操作系统 : Debian 11
- 服务器IP : 192.168.66.162

## 二、旧的云WAF服务器需要做的步骤

首先在旧的服务器进行停止云WAF与备份

使用SSH工具登录旧的服务器，执行以下命令安装：

- 注意需要ROOT权限执行命令

### 1. 停止WAF:

```
btw stop
```

```
root@old-WAF:~#  
root@old-WAF:~#  
root@old-WAF:~#  
root@old-WAF:~# btw stop  
Stopping cloudwaf_nginx... done  
Stopping cloudwaf_mysql... done  
Stopping ipfilter... done  
Stopping bt-cloudwaf... done  
root@old-WAF:~# █
```

### 2. 直接打包整个目录进行备份迁移

```
cd /www/ && tar -zcvf cloud_waf.tar.gz cloud_waf
```

```
root@old-WAF:~#  
root@old-WAF:~# cd /www/ && tar -zcvf cloud_waf.tar.gz cloud_waf  
cloud_waf/  
cloud_waf/vhost/  
cloud_waf/vhost/ssl/  
cloud_waf/vhost/ssl/156_kern123_tk/
```

备份成功后查看文件与验证md5值：

```
ls -ahl  
md5sum cloud_waf.tar.gz
```

```
root@old-WAF:/www# ls -ahl  
total 45M  
drwxr-xr-x  3 root root 4.0K Nov  6 04:07 .  
drwxr-xr-x 20 root root 4.0K Sep 20 08:14 ..  
drwxr-xr-x  7 root root 4.0K Nov  1 09:29 cloud_waf  
-rw-r--r--  1 root root  45M Nov  6 04:07 cloud_waf.tar.gz  
root@old-WAF:/www#  
root@old-WAF:/www# md5sum cloud_waf.tar.gz  
b302833275f1de127e545d043d8177d1  cloud_waf.tar.gz  
root@old-WAF:/www#
```

### 3. 下载备份文件 cloud\_waf.tar.gz

- 可以使用 Xftp、Winscp 等工具下载到本地电脑中，然后再上传到新的服务器到 `/root` 目录

注意检查下载的文件是否完整

- 或者使用 scp 命令直接远程复制到新的服务器：

注意：将“新的服务器IP” 更换成您的新服务器IP

第一次连接需要输入yes, 然后再输入新服务器的 root 密码

```
scp cloud_waf.tar.gz root@新的服务器IP:/root/
```

```
root@old-WAF:/www# scp cloud_waf.tar.gz root@192.168.66.162:/root/  
The authenticity of host '192.168.66.162 (192.168.66.162)' can't be established.  
ECDSA key fingerprint is SHA256:kv0+awwCleTdZXBSwwkGPeJ1incbyoMV0/kF1Y2+whk.  
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes  
Warning: Permanently added '192.168.66.162' (ECDSA) to the list of known hosts.  
root@192.168.66.162's password:  
cloud_waf.tar.gz 100% 45MB 85.1MB/s 00:00  
root@old-WAF:/www#
```

## 三、新的服务器需要做的步骤：

### 1.上传并且解压还原mysql文件

使用SSH工具登录 新的服务器，执行以下命令安装：

- 注意需要ROOT权限执行命令

1. 在新的服务器上确认备份文件是否存在？确认md5值是否一致？

```
cd /root/ && ls -lh && md5sum cloud_waf.tar.gz
```

```
root@NNew-WAF:~#  
root@NNew-WAF:~# cd /root/ && ls -lh && md5sum cloud_waf.tar.gz  
total 45M  
-rw-r--r-- 1 root root 45M Nov  6 12:12 cloud_waf.tar.gz  
b302833275f1de127e545d043d8177d1  cloud_waf.tar.gz  
root@NNew-WAF:~#
```

2. 解压备份文件

```
tar -zxf cloud_waf.tar.gz
```

3. 建立目录与恢复mysql数据

```
mkdir -pv /www/cloud_waf/nginx/conf.d/waf/  
  
\cp -arpf /root/cloud_waf/nginx/conf.d/waf/mysql_default.pl /www/cloud_waf/  
nginx/conf.d/waf/mysql_default.pl  
  
mv /root/cloud_waf/mysql /www/cloud_waf/mysql
```

4. 查看文件是否成功移动

```
ls /www/cloud_waf/mysql/
```

```
root@NNew-WAF:~#
root@NNew-WAF:~# tar -zxf cloud_waf.tar.gz
root@NNew-WAF:~#
root@NNew-WAF:~# mkdir -pv /www/cloud_waf/nginx/conf.d/waf/
mkdir: created directory '/www/'
mkdir: created directory '/www/cloud_waf/'
mkdir: created directory '/www/cloud_waf/nginx/'
mkdir: created directory '/www/cloud_waf/nginx/conf.d/'
mkdir: created directory '/www/cloud_waf/nginx/conf.d/waf/'
root@NNew-WAF:~#
root@NNew-WAF:~# \cp -arpf /root/cloud_waf/nginx/conf.d/waf/mysql_default.pl /www/cloud_waf/nginx/conf.d/
/waf/mysql_default.pl
root@NNew-WAF:~#
root@NNew-WAF:~# mv /root/cloud_waf/mysql /www/cloud_waf/mysql
root@NNew-WAF:~#
root@NNew-WAF:~# ls /www/cloud_waf/mysql/
conf data log
root@NNew-WAF:~#
```

## 2. 在新的服务器中安装云WAF

### 1. 新的服务器执行命令安装云WAF

```
URL=https://download.bt.cn/cloudwaf/scripts/install_cloudwaf.sh && if [ -f /usr/bin/curl ];then curl -sSO "$URL" ;else wget -O install_cloudwaf.sh "$URL";fi;bash install_cloudwaf.sh
```

```
内网访问地址: https://192.168.66.162:8379/4ed1bb68
username: ce64407c 请忽略新安装的访问地址与帐号和密码 ←
password: f1632dbc
If you cannot access the Bt-WAF
release the following Bt-WAF port [8379] in the security group
若无法访问堡塔云WAF, 请检查防火墙/安全组是否有放行[8379]端口
```

注意：这里请忽略显示的登录信息，因为下面会将旧的云WAF数据恢复到新的服务器中。

### 2. 安装成功后，等待5秒，停止云WAF

```
sleep 5 && btw stop
```

### 3. 等待5秒后，恢复旧云WAF的数据

```
sleep 5 && \cp -arpf /root/cloud_waf/* /www/cloud_waf
```

注意：查看是否有错误



#### 4. 查看文件是否成功复制

```
ls -l /www/cloud_waf
```

#### 5. 启动云WAF

```
btw start
```

注意: 检查是否启动成功

```
root@NNew-WAF:~#
root@NNew-WAF:~# sleep 5 && btw stop
Stopping cloudwaf_nginx... done
Stopping cloudwaf_mysql... done
Stopping ipfilter... done
Stopping bt-cloudwaf... done
root@NNew-WAF:~# sleep 5 && \cp -arpf /root/cloud_waf/* /www/cloud_waf
root@NNew-WAF:~# ls -l /www/cloud_waf
total 120
-rw-r--r--  1 root root 37206 Sep 19 16:43 btw.init
-rw-r--r--  1 root root   363 Sep 11 14:31 btw.service
-rw-r--r--  1 root root 53508 Sep 20 17:14 cloudwaf_check.sh
drwxr-xr-x  7 root root  4096 Nov  1 17:29 console
drwxr-xr-x  5 root root  4096 Sep  5 10:16 mysql
drwxr-xr-x  5 root root  4096 Sep  5 10:16 nginx
drwxr-xr-x  6 root root  4096 Sep 26 14:41 vhost
drwxr-xr-x 11 root root  4096 Sep  6 10:34 wwwroot
root@NNew-WAF:~# btw start
Starting cloudwaf_nginx... done
Starting cloudwaf_mysql... done
Starting ipfilter... done
Starting bt-cloudwaf... done
root@NNew-WAF:~# █
```

### 3. 登录新的云WAF

查看云WAF登录地址信息，可以查看到仅更换了IP，其他信息没有改变。

```
btw 6
```

```
root@NNew-WAF:~# btw 6
=====
以下是堡塔云WAF登录地址!
=====
外网访问地址: https://          :8379/5f0eb9aa
内网访问地址: https://192.168.66.162:8379/5f0eb9aa
username: 5c32ce9b
password: *****
如果您忘记了密码, 请执行btw 9手动重置密码或btw 10重置随机密码
若无法访问堡塔云WAF, 请检查防火墙/安全组是否有放行[8379]端口
=====
```

使用显示的登录地址来登录云WAF

如: <https://192.168.66.162:8379/5f0eb9aa>

注意: 请使用旧的云WAF帐号与密码进行登录, 如果忘记了可以使用 `btw 10` 命令重置密码

## 4.检查云WAF功能是否正常?

如何检查: 可以检查旧的云WAF有数据的界面, 比如

- 首页概览
- 拦截日志
- 操作日志
- 网站列表

拦截日志:

访问时间	状态	域名	URI	攻击IP	IP归属地	攻击类型	操作
2023-11-01 16:49:12	已拦截	156.kern123.tk	//id=/etc/passwd	192.168.168.163	内网地址	文件包含防御	拦截 加白URL 详情
2023-10-31 14:47:22	已拦截	156.kern123.tk	//id=/etc/passwd	192.168.168.163	内网地址	文件包含防御	拦截 加白URL 详情
2023-10-31 14:47:07	已拦截	156.kern123.tk	//id=/etc/passwd	192.168.168.163	内网地址	文件包含防御	拦截 加白URL 详情
2023-10-27 11:31:46	已拦截	156.kern123.tk	//id=/etc/passwd	192.168.168.163	内网地址	文件包含防御	拦截 加白URL 详情

如果不正常将无数据显示 或者 请求出错, 请稍后再试

在新的云WAF中执行 `btw 18` 命令检查是什么原因导致的

正常请继续下一步

## 5.检查网站是否正常?

首先将域名的A记录解析的IP 更换为 新服务器的IP

- 即将 旧的云WAF服务器IP: 192.168.66.156 更换为新的云WAF服务器IP: 192.168.66.162
- 等待解析生效后测试访问您的域名，如: <http://nw1.kern123.tk>

通过以下方式查看新的云WAF服务器是否有生效:

- 首页概览 --> 今日请求数
- 网站列表 --> 今日访问/拦截
- 网站列表 相关域名 的日志是否有内容

如果没有记录，建议检查更换的域名A记录解析是否生效？解析记录是否正确？

网站是否正常需要您自行检查，可以随意点击几个功能来测试是否正常

如果没有问题，这么迁移就完成了。

确认没有问题后，您可以选择删除解压出来的文件了，同时建议保留备份压缩文件。

```
rm -rf /root/cloud_waf
```

## 教程总结

- 旧的云WAF服务器：

1. 停止云WAF
2. 备份云WAF
3. 下载备份文件

- 新的云WAF服务器

1. 上传备份文件
2. 解压备份文件
3. 建立相关目录
4. 恢复mysql数据
5. 安装云WAF
6. 停止云WAF



7. 恢复云WAF
8. 启动云WAF
9. 检查云WAF是否正常
10. 更换域名A记录解析
11. 检查网站是否正常

## 如果是同一台服务器，需要重新安装操作系统如何备份恢复？

不需要：更换域名A记录解析

基本上与迁移到新的服务器相同

- 在云WAF服务器操作流程：
  1. 停止云WAF
  2. 备份云WAF
  3. 下载备份文件
  4. 重新安装操作系统
  5. 上传备份文件
  6. 解压备份文件
  7. 建立相关目录
  8. 恢复mysql数据
  9. 安装云WAF
  10. 停止云WAF
  11. 恢复云WAF
  12. 启动云WAF
  13. 检查云WAF是否正常
  14. 检查网站是否正常

## 不同的系统架构如何迁移？

如：x86\_64 迁移到 aarch64

只需在 启动云WAF：`btw start` 之前执行更新命令 `btw 17` 更新一次即可，会自动下载相应的架构文件覆

盖。

如果不更新会出错无法启动，错误信息：`/www/cloud_waf/console/CloudWaf: cannot execute binary file:  
Exec format error`

如使用中有问题，请联系我们：

加入微信讨论群



# 动态口令认证-二步认证

---

- [如何使用动态口令认证](#)
  - [先下载安装手机APP或者打开](#)
  - [开启动态口令认证](#)
    - [设置 --> 动态口令认证](#)
  - [登录](#)
  - [关闭动态口令认证](#)

## 如何使用动态口令认证

### 先下载安装手机APP或者打开

---

- [Google Authenticator \(身份验证器\)](#)
- [Microsoft Authenticator](#)
- [微信：腾讯身份验证器小程序](#)

( 选择任一身份验证器 )

### 开启动态口令认证

---

#### 设置 --> 动态口令认证

1. 在 [了解详情](#) 后点击确定开启



## 2. 开启后使用 身份验证器 进行扫码绑定



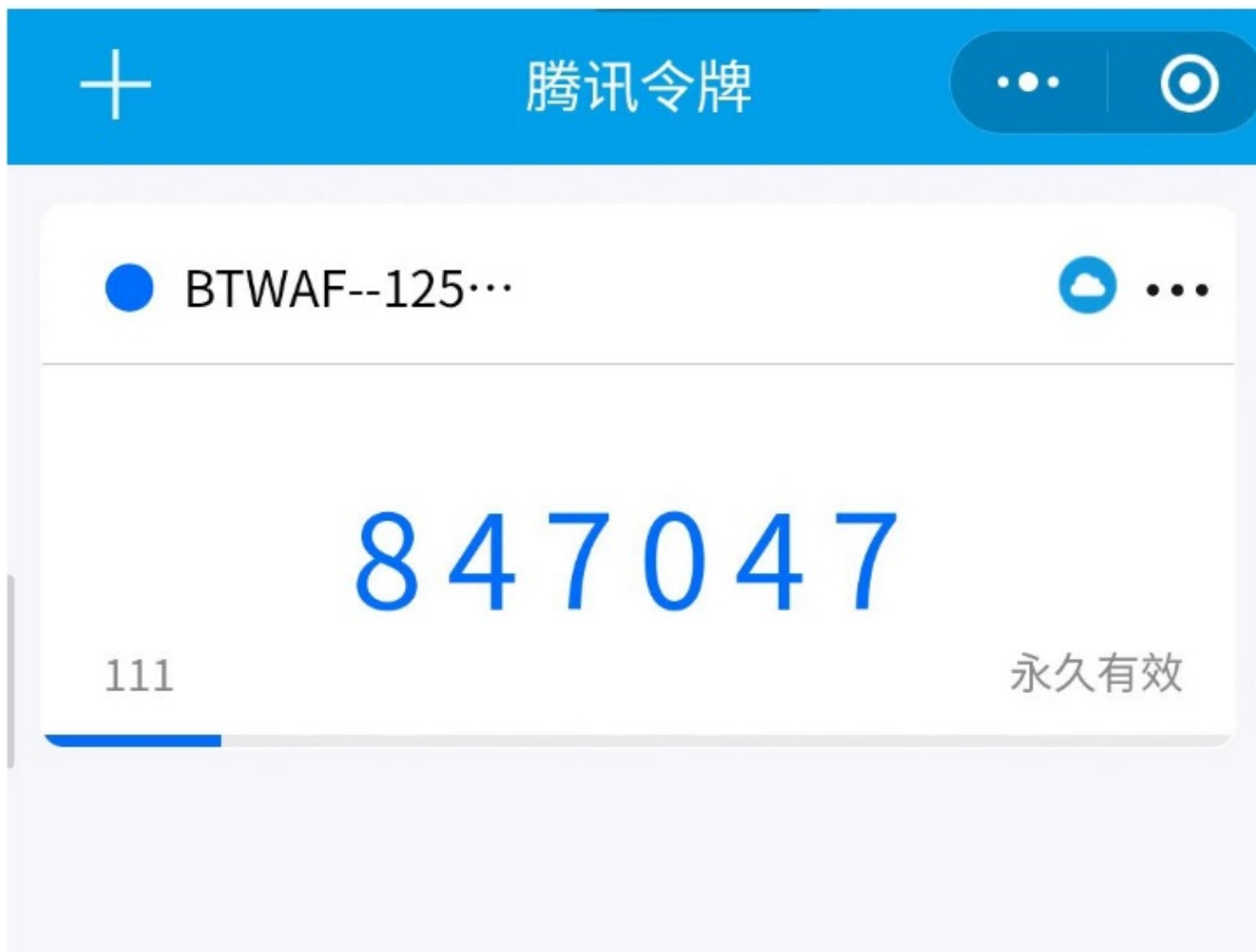
3. 扫码绑定成功后测试，点击 退出 退出登录

## 登录

1. 在登录界面 输入帐号密码 进行登录，会弹出需要动态口令



2. 打开 身份验证器 查看动态口令，并且在过期前 输入正确的动态口令 进行登录



3. 登录成功会跳转到首页概览

## 关闭动态口令认证

使用SSH工具连接到服务器执行命令

注意需要ROOT权限执行命令，记得按回车键喔

```
btw 16
```

关闭成功：

```
[root@waf-centos9 ~]# btw 16  
正在关闭动态口令认证...  
关闭动态口令成功!  
Stopping bt-cloudwaf... done  
Starting bt-cloudwaf... done  
[root@waf-centos9 ~]#
```

# 常用命令

注意 btw 后面都有一个空格然后是参数。如：btw 6

需要ROOT权限执行命令

- 常用命令

- 查看堡塔云WAF管理界面登录地址、用户信息
- 仅重启堡塔云WAF管理界面(不影响网站访问)
- 查看堡塔云WAF运行状态
- 修改管理员密码
- 修改管理员用户名
- 仅重启nginx
- 重启整个堡塔云WAF，会影响网站的访问
- 取消域名绑定
- 取消IP绑定限制
- 关闭动态口令认证
- 在线修复、更新堡塔云WAF
- 检查堡塔云WAF是否有错误
- 查看堡塔云WAF日志
- 停止堡塔云WAF
- 查看更多命令

## 常用命令

查看堡塔云WAF管理界面登录地址、用户信息

```
btw 6
```

仅重启堡塔云WAF管理界面(不影响网站访问)

```
btw 2
```

查看堡塔云WAF运行状态



```
btw 3
```

## 修改管理员密码

---

```
btw 9
```

## 修改管理员用户名

---

```
btw 11
```

## 仅重启nginx

---

```
btw nginx_restart
```

## 重启整个堡塔云WAF，会影响网站的访问

---

```
btw 1
```

## 取消域名绑定

---

```
btw 14
```

## 取消IP绑定限制

---

```
btw 15
```

## 关闭动态口令认证

---

```
btw 16
```

## 在线修复、更新堡塔云WAF

---

```
btw 17
```

## 检查堡塔云WAF是否有错误

---

```
btw 18
```

## 查看堡塔云WAF日志

---

```
btw 5
```

## 停止堡塔云WAF

---

```
btw 4
```

## 查看更多命令

---

```
btw h
```

# 更新日志

---

- [堡塔云WAF 更新日志](#)

- [2024-01-19 V3.1 正式版本](#)
- [2024-01-15 V3.0 正式版本](#)
- [2024-01-03 V2.9 正式版本](#)
- [2023-12-28 V2.8 正式版本](#)
- [2023-12-20 V2.7 正式版本](#)
- [2023-12-14 V2.6 正式版本](#)
- [2023-12-05 V2.5 正式版本](#)
- [2023-11-29 V2.4 正式版本](#)
- [2023-11-28 V2.3 正式版本](#)
- [2023-11-21 V2.2 正式版本](#)
- [2023-11-15 V2.1 正式版本](#)
- [2023-11-10 V2.0 正式版本](#)
- [2023-11-06 V1.9 正式版本](#)
- [2023-11-04 V1.8 正式版本](#)
- [2023-11-01 V1.7 正式版本](#)
- [2023-10-26 V1.6 正式版本](#)
- [2023-10-25 V1.5 正式版本](#)
- [2023-10-21 V1.4 正式版本](#)
- [2023-10-13 V1.3 正式版本](#)
- [2023-09-26 V1.2 正式版本](#)
- [2023-09-21 V1.1 正式版本](#)
- [2023-09-20 V1.0 正式版本](#)
- [2023-09-14 V0.1 内测版本](#)

## 堡塔云WAF 更新日志

### 2024-01-19 V3.1 正式版本

---

【新增】添加网站 - 增加通配【\*】所有域名支持

【新增】回源配置 - 回源域名解析巡检

【新增】访问域名不存在时，显示网站不存在页面

【修复】卸载重装后绑定账号不会自动恢复授权的BUG

【修复】已知BUG

## 2024-01-15 V3.0 正式版本

---

【修复】云WAF一处SQL注入BUG

## 2024-01-03 V2.9 正式版本

---

【新增】网站日志 - [日志管理]/[清空日志]

【新增】拦截日志 - 规则命中记录 - [设置记录类型]

【修复】已知BUG

## 2023-12-28 V2.8 正式版本

---

【新增】[网站配置] - 新增常用参数配置

【新增】[网站列表] - [禁止中国境外地区访问]

【优化】文件大小上传

【优化】XSS引擎拦截

【优化】文件上传检测引擎拦截

【优化】允许用户设置[服务器]在[攻击地图]中的[所在地]

【修复】[网站配置] - 全局规则不会自动继承到新建网站

【修复】网站已有证书时再保存报错

【修复】网站加速在开启了gzip压缩的场景下文本乱码的BUG

【修复】规则命中记录会记录127.0.0.1的问题

【修复】已知BUG

## 2023-12-20 V2.7 正式版本

---

【新增】攻击大屏

【新增】[自定义规则] - [自定义cc防御] -- 人机验证

- 【修复】系统流量不刷新问题
- 【优化】基础CC拦截效果大幅度提升
- 【修复】已知BUG

## 2023-12-14 V2.6 正式版本

---

- 【调整】更新WAF程序使用的IP库
- 【修复】控制台异常崩溃问题
- 【修复】XSS误拦截问题
- 【优化】提升控制台WEB服务性能
- 【修复】已知BUG

## 2023-12-05 V2.5 正式版本

---

- 【新增】[网站配置]响应内容关键字替换
- 【新增】[概览页]系统流量监控图表
- 【新增】[添加网站]端口占用检测--仅检测waf端口转发占用的端口
- 【新增】[自定义规则]新增user-agent、referer匹配条件
- 【新增】[自定义规则] - [自定义cc防御]
- 【新增】开启CDN后自动获取真实客户端IP并写入访问日志
- 【修复】docker崩溃生成coredump导致磁盘空间不足的问题
- 【修复】waf端在某些场景下CPU跑满的BUG
- 【修复】[ssl证书]证书配置部署状态
- 【优化】[添加网站]回源地址输入交互

## 2023-11-29 V2.4 正式版本

---

- 【优化】进一步减少[自定义规则]waf性能开销
- 【修复】[端口转发]--某些情况下设置失败BUG

【修复】[端口转发]--转发次数不准确BUG

【修复】[网站加速]--某些情况无法正常加速静态资源的BUG

【修复】已知BUG

## 2023-11-28 V2.3 正式版本

---

【新增】[自定义规则]-可以根据各种条件制定拦截、放行规则

【新增】证书可以引用到网站的自定义端口

【新增】添加源站地址时增加域名支持

【新增】开启动态口令认证时支持指定密钥

【优化】[拦截日志]--加白url匹配条件调整为同时匹配网站名、请求方式、参数名

【优化】[网站加速]--调整为仅加速静态资源，同时大幅优化加速性能

【修复】已知BUG

## 2023-11-21 V2.2 正式版本

---

注意：

本次升级将升级 cloudwaf\_nginx 容器版本为 nginx-openresty/1.21.4.3 ，修复NGINX HTTP/2处理中的安全漏洞(C-2023-4487)

建议使用ssh工具登录服务器执行：`btw 17` 命令进行升级。

升级过程中网站无法访问，建议在用户访问量少时升级，预计需要 1-2 分钟。

1. 【新增】IP组（可用功能：IP黑白名单、人机验证）
2. 【优化】访问地图 可查看今天、昨天、近7天、近30天
3. 【优化】[网站列表]添加网站时进行端口检测
4. 【优化】[WAF]基础函数执行效率
5. 【修复】[网站加速]命中率大于100%的问题
6. 【修复】[WAF]CPU与内存占用异常过高的问题
7. 【修复】[规则命中记录]列表获取失败问题

## 2023-11-15 V2.1 正式版本

---

1. 【新增】端口转发
2. 【新增】网站设置-模拟攻击
3. 【新增】网站设置-文件路径保护-网站后台入口保护
4. 【优化】网站列表 - 网站日志显示
5. 【优化】WAF性能
6. 【兼容】ARM架构
7. 【修复】已知BUG

## 2023-11-10 V2.0 正式版本

---

1. 【新增】网站加速
2. 【新增】设置--自定义LOGO与拦截页面功能
3. 【新增】地区限制--“中国(包括[中国特别行政区:港,澳,台])”常用选项
4. 【新增】编辑、删除回源节点时检测http协议并更新
5. 【新增】网站设置增加一键恢复默认防护配置
6. 【修复】添加域名时加入特殊端口无法开启证书BUG
7. 【修复】WAF程序误拦截BUG
8. 【修复】WAF程序CPU占用持续上升问题
9. 【修复】已知BUG

## 2023-11-06 V1.9 正式版本

---

1. 【新增】页面左上角新增【需求反馈】提交功能
2. 【优化】语义分析引擎
3. 【优化】调整防护描述
4. 【优化】【回源负载均衡】调整为公测状态，所有用户都可以使用
5. 【修复】拦截日志 -- 规则命中记录状态显示错误
6. 【修复】已知BUG

## 2023-11-04 V1.8 正式版本

---

1. 【新增】《堡塔恶意IP共享计划》
2. 【新增】回源负载均衡
3. 【新增】网站监听ipv6
4. 【新增】全局规则和站点规则--命令执行拦截
5. 【新增】站点规则--护网防护
6. 【新增】全局规则-拦截恶意IP访问
7. 【优化】地区限制命中记录
8. 【修复】价格页原价显示BUG

## 2023-11-01 V1.7 正式版本

---

1. 【优化】基础CC防御
2. 【优化】添加网站--防护域名检测
3. 【优化】概览页--攻击地图
4. 【优化】F11全屏效果
5. 【修复】概览页--请求数据重复刷新问题
6. 【修复】添加网站--多域名添加BUG
7. 【修复】添加网站--防护域名检测CDN状态不准确BUG
8. 【修复】添加网站--检测源站地址BUG
9. 【修复】网站配置--gzip不生效BUG
10. 【修复】PHP检测导致的CPU满载问题
11. 【修复】SQL注入误报问题

## 2023-10-26 V1.6 正式版本

---

1. 【优化】动态口令--兼容大部分APP
2. 【优化】网站列表--提升列表加载速度
3. 【优化】黑白名单--大幅提升导入速度
4. 【修复】规则命中记录--清空日志BUG
5. 【修复】添加网站--泛域名丢失通配符
6. 【修复】设置--关闭在线客服悬浮框BUG
7. 【修复】人机验证--删除BUG
8. 【修复】黑白名单--删除BUG
9. 【修复】已知BUG



## 2023-10-25 V1.5 正式版本

---

1. 【新增】添加网站--防护域名检测
2. 【新增】添加网站--源站地址检测
3. 【新增】拦截日志--规则命中记录
4. 【新增】全局规则--搜索框
5. 【优化】添加网站UI界面交互
6. 【修复】控制台因为致命BUG导致的进程终止
7. 【修复】拦截日志--CC攻击事件持续时间负数BUG
8. 【修复】已知BUG

## 2023-10-21 V1.4 正式版本

---

1. 【新增】URI地区限制
2. 【新增】拦截日志--CC攻击事件
3. 【新增】设置页--显示/隐藏在线客服
4. 【优化】WAF规则匹配优先级
5. 【优化】全局通用规则可选择应用到指定网站
6. 【优化】修改控制台端口后自动放行对应端口
7. 【优化】防护域名自定义端口时自动放行对应端口
8. 【优化】拦截页面样式
9. 【优化】人机验证样式
10. 【优化】命中次数样式
11. 【修复】动态CC误判API的BUG
12. 【修复】已知BUG

## 2023-10-13 V1.3 正式版本

---

1. 【新增】免费领取14天专业版试用
2. 【新增】首页攻击地图新增切换设置
3. 【新增】全屏功能
4. 【新增】地区限制、黑白名单新增清空统计

5. 【新增】控制台会话超时时间设置
6. 【新增】单站点IDC访问限制-付费功能
7. 【新增】网站SSL自定义加密套件和安全协议
8. 【新增】地区限制重置命中次数
9. 【优化】融合网站配置和独立规则
10. 【优化】命中次数展示
11. 【优化】拦截日志新增[全部]展示
12. 【优化】NGINX各超时配置为600s
13. 【优化】网站日志切割增加重载机制
14. 【优化】优化域名检测
15. 【修复】登录验证码区分大小写的BUG
16. 【修复】购买后授权信息没有立即刷新的BUG
17. 【去除】网站配置去除proxy\_http\_version配置

## 2023-09-26 V1.2 正式版本

---

1. 【优化】首页访问加载
2. 【优化】部分删除提示
3. 【优化】操作日志详情
4. 【优化】网站日志切割
5. 【优化】网站列表去除端口显示

## 2023-09-21 V1.1 正式版本

---

1. 【优化】黑白名单命中次数统计
2. 【优化】网站列表--兼容"域名:端口"格式添加网站
3. 【优化】防御模块提升稳定性
4. 【修复】动态口令登录不跳转BUG
5. 【修复】删除人机验证规则后，总数不更新的BUG
6. 【修复】全局规则--应用到所有网站bug

## 2023-09-20 V1.0 正式版本

---

- 【优化】 首页大屏

更新日志

【优化】 拦截显示

2023-09-14 V0.1 内测版本

---

【新增】 上线堡塔云WAF

# 堡塔云WAF集群版

---

[产品简介](#)

[工作原理](#)

[安装主控](#)

[添加防护网站](#)

[安装被控](#)

[更新日志](#)

# 产品简介



## 堡塔云WAF

btwaf BTWAF openresty luajit release v3.1 Stars 28

### 堡塔云WAF

免费的私有云WAF防火墙

堡塔云WAF经过千万级用户认证，为您的业务保驾护航，免费私有云WAF防火墙，有效拦截sql注入、xss、一句话木马、防采集等常见渗透攻击，为您的业务网站保驾护航。

## 演示站(Demo)

<https://btwaf-demo.bt.cn:8379/c0edce7a>

## 立即安装

推荐使用此安装方式

使用SSH工具登录服务器，执行以下命令安装主控：

- 注意需要ROOT权限执行命令

复制粘贴命令后，按回车执行命令安装主控

```
URL=https://download.bt.cn/cloudwaf/scripts/install_waf_master.sh && if [ -f /usr/bin/curl ];then curl -sSO "$URL" ;else wget -O install_waf_master.sh "$URL";fi;bash install_waf_master.sh
```

[点击查看：堡塔云WAF系统兼容表](#)

## 加入微信讨论群

---



# 工作原理

## 堡塔云WAF工作原理

堡塔云WAF是由三个主要组件构成：

- cloudwaf\_nginx（简称为nginx）用于检查和过滤恶意流量，并将流量转发给网站服务器。
- cloudwaf\_mysql（简称为mysql）用于存储攻击事件日志。
- CloudWaf 是堡塔云WAF的管理程序，提供管理界面供用户使用（简称为管理程序）。

它如何工作的？

堡塔云WAF以反向代理的方式工作。网站流量先抵达堡塔云WAF，经过堡塔云WAF检测和过滤后，再转给原来提供服务的网站服务器。

堡塔云WAF集群由 **主控** 与 **被控** 组成。

- 主控：提供管理界面用于管理网站，同步设置到被控，查看、接收被控拦截、访问量等数据。
- 被控：提供网站防护，接收主控设置，记录拦截日志，访问量等数据，没有管理界面。

示例

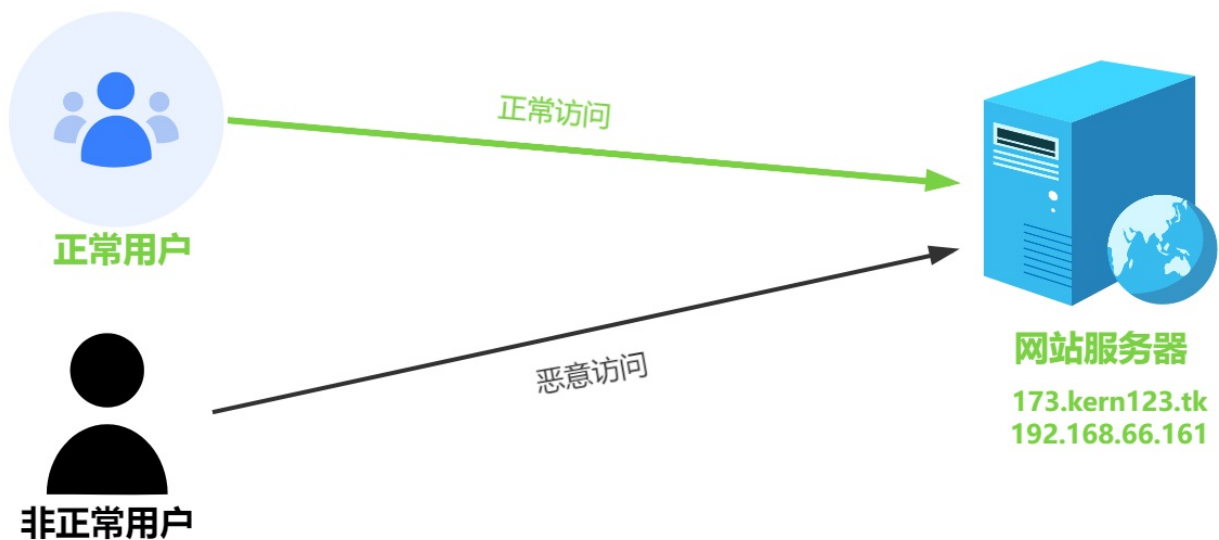
通过一个简单的例子描述如何搭建堡塔云WAF

未接入堡塔云WAF前

所有用户的流量直接流向提供网站的服务器

- 网站域名：[173.kern123.tk](http://173.kern123.tk)
- 网站服务器IP、网站域名A记录IP：192.168.66.161

如图：

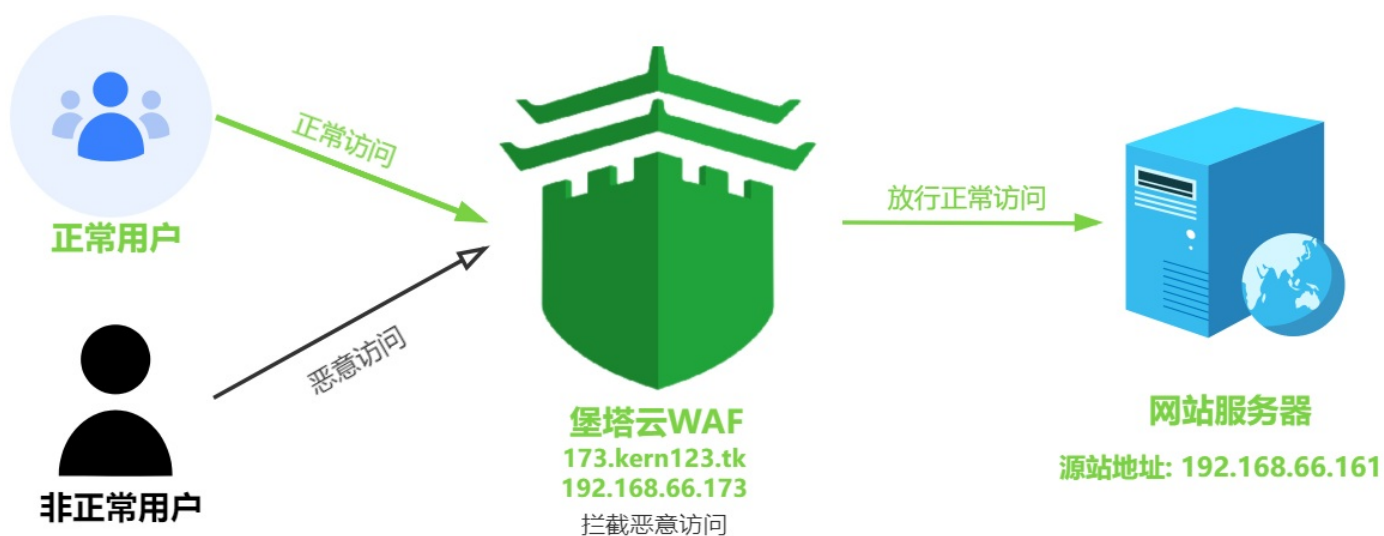


接入堡塔云WAF后

所有用户的流量先流向堡塔云WAF通过WAF过滤恶意流量后再将正常流量发送到源站服务器（网站服务器在这也称回源服务器，简称：源站地址）。

- 防护网站（网站域名）：[173.kern123.tk](http://173.kern123.tk)
- 堡塔云WAF、防护网站A记录IP：192.168.66.173
- 网站服务器IP（源站地址）：192.168.66.161

如图：





# 安装主控

## 主控安装方式

[点击查看：堡塔云WAF系统兼容表](#)

温馨提示：中国内地（大陆）服务器需要备案，建议您在已经备案的服务商上购买新的服务器，否则需要重新接入备案。

可参考阿里云：[接入备案流程](#)

### 在线安装主控

推荐使用此安装方式

使用SSH工具登录服务器，执行以下命令安装主控：

- 注意需要ROOT权限执行命令

复制粘贴命令后，按回车执行命令安装主控

```
URL=https://download.bt.cn/cloudwaf/scripts/install_waf_master.sh && if [ -f /usr/bin/curl ];then curl -sSO "$URL" ;else wget -O install_waf_master.sh "$URL";fi;bash install_waf_master.sh
```

```
root@Master:~#  
root@Master:~# URL=https://download.bt.cn/cloudwaf/scripts/install_waf_master.sh && if [ -f /usr/bin/curl ];then curl -sSO "$URL" ;else wget -O install_waf_master.sh "$URL";fi;bash install_waf_master.sh
```

主控安装完成后显示以下信息

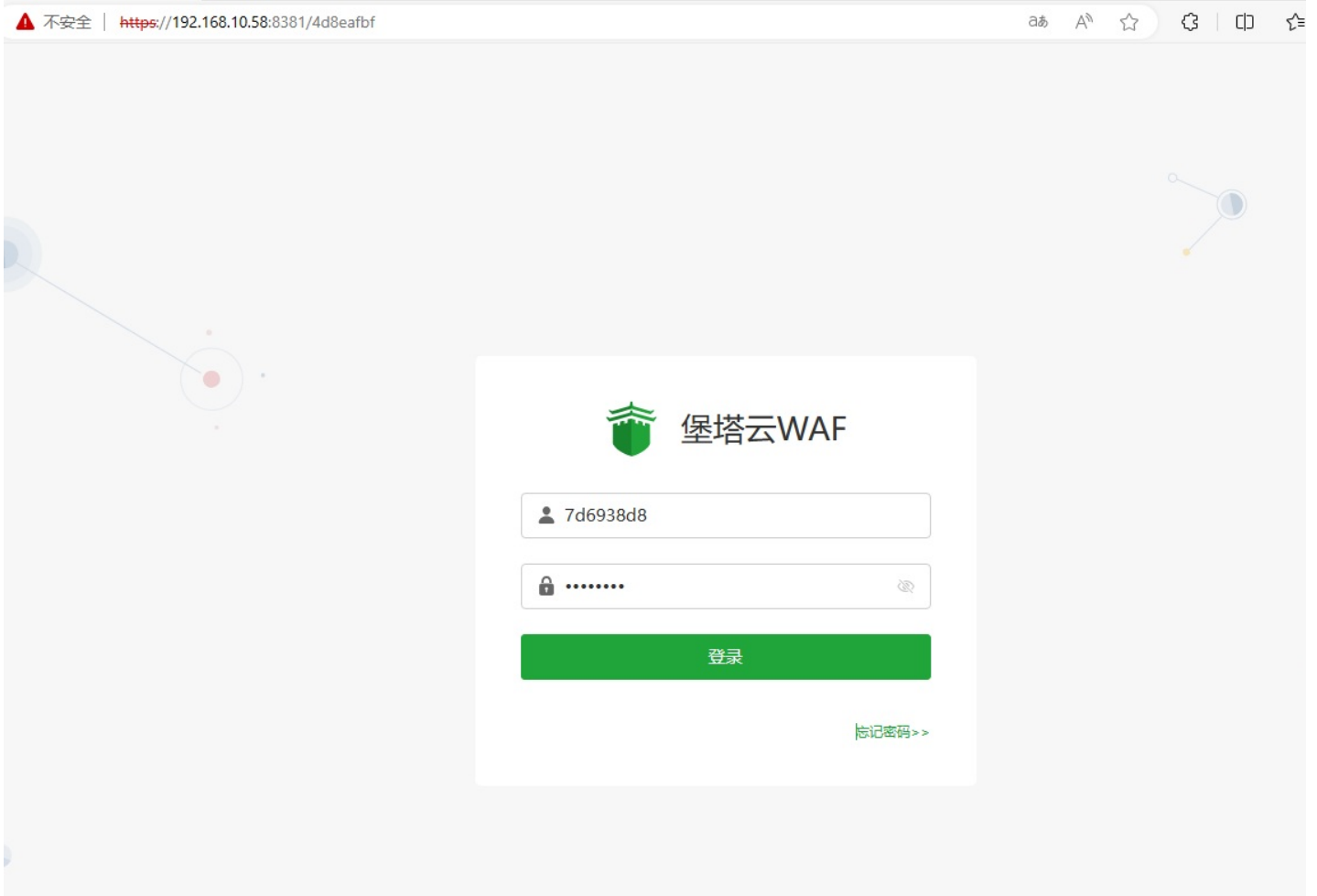
```
正在导入数据中,请耐心等待...
Restarting cloudwaf_nginx... done
Stopping ipfilter... done
Starting ipfilter... done
Stopping bt-cloudwaf... done
Starting bt-cloudwaf... done
正在检查堡塔云WAF集群主控初始化状态中,请稍等...
堡塔云WAF集群主控初始化中,1/30次后将自动退出,10秒后再检查...
Synchronizing state of btw.service with SysV service script with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable btw
Command may disrupt existing ssh connections. Proceed with operation (y|n)? Firewall is active and enabled
Default incoming policy changed to 'deny'
(be sure to update your rules accordingly)
Firewall reloaded
=====
堡塔云WAF集群主控安装完成! Installed successfully!
=====
外网访问地址: https://125.93.252.236:8381/4d8eafbfbf
内网访问地址: https://192.168.10.58:8381/4d8eafbfbf
username: 7d6938d8
password: 2557a3ba
If you cannot access the WAF-Master
release the following WAF-Master port [8381,80,443] in the security group
若无法访问堡塔云WAF集群主控, 请检查防火墙/安全组是否有放行[8381,80,443]端口
=====打开堡塔云WAF集群主控前请看=====
因默认启用自签证书https加密访问, 浏览器将提示不安全
点击【高级】-【继续访问】或【接受风险并继续】访问
参考教程: https://www.bt.cn/bbs/thread-117246-1-1.html
=====
Time consumed: 1 Minute!
```

## 登录主控管理界面

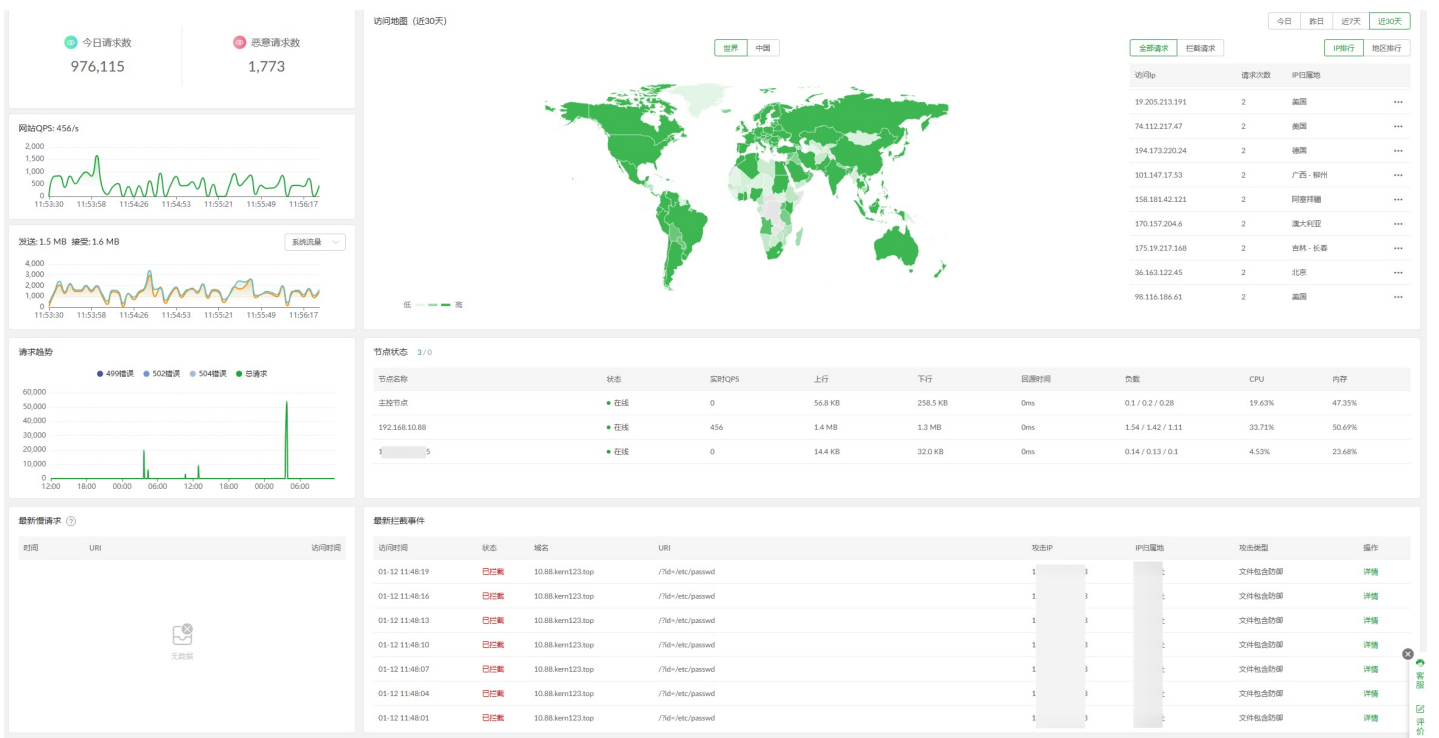
主控默认端口8381, 如果服务器有安全组、硬件防火墙, 请开放8381端口

安装完成后, 使用浏览器访问显示的地址, 输入账号(username)与密码(password), 登录主控管理界面

注意: 浏览器提示安全问题, 请信任它。因为自签证书浏览器不信任导致的



## 登录成功后即可使用堡塔云WAF集群版



## 离线安装主控

注意，此安装方式适用于服务器无法连接公网节点时的选择

- 离线安装时必须手动安装 docker，否则无法安装
- 离线安装前请确保您的服务器存在 tar gzip curl netstat ss docker 命令，可以使用此命令检查是否存在：

```
Packs=("curl" "tar" "gzip" "netstat" "ss" "docker" ); for pack in "${Packs[@]}";  
do command -v "$pack" >/dev/null 2>&1 || echo -e "\033[31mError: $pack 命令不存  
在\033[0m"; done
```

请根据您的系统架构下载安装文件，使用命令 `uname -m` 可以查看架构

x86\_64 架构：

- 离线安装脚本：[点击下载离线安装脚本](#)
- 下载镜像文件：[点击下载镜像 x86\\_64 架构文件](#)
- 下载cloudwaf程序文件：[点击下载cloudwaf程序 x86\\_64 架构文件](#)

aarch64 架构：

- 离线安装脚本：[点击下载离线安装脚本](#)
- 下载镜像 aarch64 架构文件：[点击下载镜像 aarch64 架构文件](#)
- 下载cloudwaf程序 aarch64 架构文件：[点击下载cloudwaf程序 aarch64 架构文件](#)

根据不同的系统架构下载文件后，使用Xftp、Winscp等工具上传到服务器中，将下载的文件放在相同的路径，然后执行安装命令离线安装主控：

注意需要ROOT权限执行命令

```
bash install_waf_master.sh offline
```

安装完成后，登录步骤与在线相同 示例为：x86\_64 架构

```
root@Master:~/cc#  
root@Master:~/cc# ls -al  
total 231676  
drwxr-xr-x  2 root root    4096 Jan 12 11:27 .  
drwx----- 11 root root    4096 Jan 12 11:27 ..  
-rw-r--r--  1 root root 192053434 Jul  7  2023 btwaf_mysql_openresty-latest.tar.gz  
-rw-r--r--  1 root root    90160 Jan 11 15:52 install_waf_master.sh  
-rw-r--r--  1 root root 45076321 Jan 12 11:26 waf-cluster-latest.tar.gz  
root@Master:~/cc#  
root@Master:~/cc# bash install_waf_master.sh offline
```

- 主控安装方式

- [点击查看：堡塔云WAF系统兼容表](#)
- [在线安装主控](#)
- [登录主控管理界面](#)
- [登录成功后即可使用堡塔云WAF集群版](#)
- [离线安装主控](#)
- 请根据您的系统架构下载安装文件，使用命令 `uname -m` 可以查看架构

# 添加防护网站

---

## 添加防护网站

环境介绍：

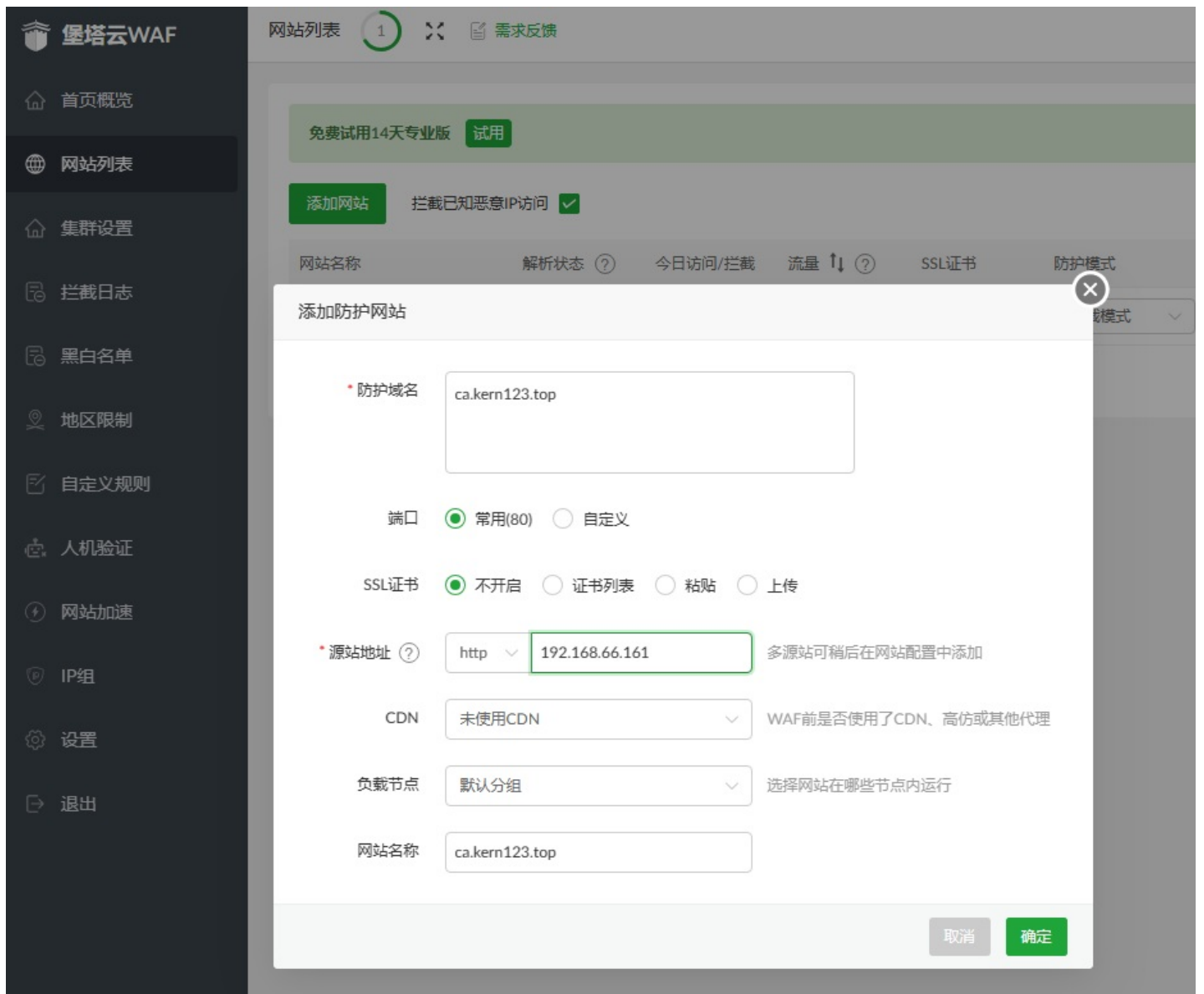
- 主控：192.168.10.58
- 网站服务器（源站地址）：192.168.66.161

网站域名	解析记录
ca.kern123.top	192.168.10.58

## 添加网站集群

---

将 ca.kern123.top 网站添加到主控节点



添加完成后，可以查看网站域名的解析状态



如果解析状态是异常或者未解析。可能有以下原因:

1. 网站域名未解析到节点IP (被控IP)
  - 请到域名提供商处，添加或者修改为 节点IP
2. 主控无法解析地址
  - 如果已经正确的解析到节点IP (被控IP)，可以忽略它
3. 域名使用了CDN
  - 如果CDN，已经配置为节点IP (被控IP)，可以忽略它

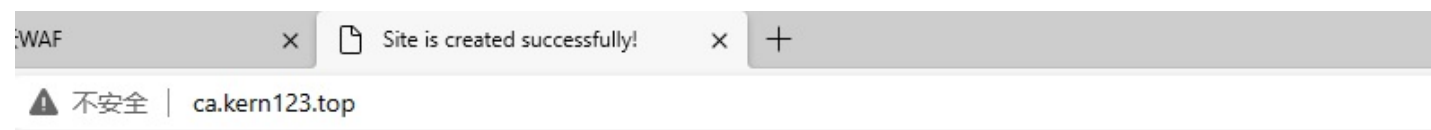
如果您的域名使用 腾讯云，阿里云 可以在主控上接入 DNS接管 一键解析 到 被 控的IP。

这里的 记录值 数据与 网站配置 -- 网站负载节点配置 设置的 负载分组 中的 节点数 一致 (如果想修改 负载分组 的节点，请在 集群设置 -- 负载均衡设置 进行修改)

记录值 的内容与 节点IP 一致，可以在 集群设置 -- 节点列表 -- 找到相关节点 (被控) 进行修改为您为客户提供服务的IP (一般是服务器外网IP)

可以使用此网站检查域名是否解析到 节点IP (被控IP) : <https://tool.chinaz.com/dns/>

使用浏览器访问 : <http://ca.kern123.top/>



**网站域名：ca.kern123.top**

测试主控节点防护是否生效，使用浏览器访问 : <http://ca.kern123.top/?id=/etc/passwd>





### 请求存在威胁，已被拦截

抱歉您的请求似乎存在威胁或带有不合法参数，  
已被管理员设置的拦截规则所阻断，请检查提交内容或联系网站管理员处理

安全检测能力由 [堡塔云WAF](#) 提供

## 添加一台被控

安装被控，请参考：[安装被控](#)

完成安装被控的环境：

- 主控：192.168.10.58
- 被控：192.168.10.80
- 网站服务器（源站地址）：192.168.66.161

网站域名	解析记录
ca.kern123.top	192.168.10.58
ca.kern123.top	192.168.10.80

再次查看网站域名的解析状态



等待1-5分钟左右，会将主控的相关配置同步到被控（会根据 **网站配置** 的 **网站负载节点配置** 设置的 **负载分组** 同步配置）。

在新添加的被控上执行命令，查看网站 ca.kern123.top 的配置。请将 ca.kern123.top 更换为您的网站域名

```
btw site_conf ca.kern123.top
```

绑定 hosts 指定网站域名,测试新添加的节点。

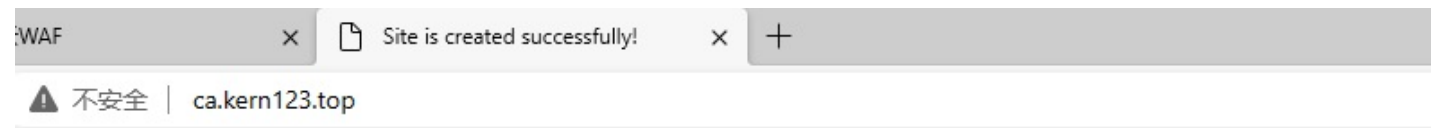
不同的操作系统 hosts 文件路径不一样：

- Windows: C:\Windows\System32\drivers\etc\hosts  
( Windows 因权限问题，无法直接修改，可以先将hosts文件复制到桌面，再修改并且保存，最后覆盖回 C:\Windows\System32\drivers\etc )
- Linux: /etc/hosts

在文件内添加并且保存：

```
192.168.10.80 ca.kern123.top
```

最后使用浏览器访问网站域名：<http://ca.kern123.top/>



网站域名: ca.kern123.top

测试主控节点防护是否生效，使用浏览器访问：<http://ca.kern123.top/?id=/etc/passwd>



请求存在威胁，已被拦截

抱歉您的请求似乎存在威胁或带有不合法参数，  
已被管理员设置的拦截规则所阻断，请检查提交内容或联系网站管理员处理

安全检测能力由 堡塔云WAF 提供

在新添加的被控上执行命令，查看网站 ca.kern123.top 的日志

```
btw site_log ca.kern123.top
```

```
root@Slave-10-80:~# btw site_log ca.kern123.top
ca_kern123_top log:
192.168.168.163 - - [11/Jan/2024:12:25:08 +0000] "GET / HTTP/1.1" 304 0 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/120.0.0.0 Safari/537.36 Edg/120.0.0.0"
内容来自于: /www/cloud_waf/nginx/logs/ca_kern123_top.log
```

有新的访问日志，被控添加已经验证完成。

- [添加防护网站](#)
  - [添加网站集群](#)
- [添加一台被控](#)
  - [绑定 hosts 指定网站域名,测试新添加的节点。](#)

# 安装被控

## 被控安装方式

在主控界面获取被控安装命令：

集群设置 --> 添加节点

在 **主控IP** 方框处，输入您的 **主控IP** 。我输入的是 192.168.10.58，然后点击 **获取命令**，最后点击 **复制** **复制安装被控命令**

(请根据您的主控、被控 网络环境输入主控IP。被控必须可以连接到主控，否则将无法安装。)

堡塔云WAF 集群设置 2 需求反馈

节点列表 DNS接管 负载均衡设置

添加节点 剩余可用授权: 0

节点名称	状态	实时QPS	上行	下行	回源时
主控节点	● 在线	188	112.85 KB	183.84 KB	

添加新节点

- 复制节点安装命令，登录到被控服务器安装节点  
主控IP  获取命令  
URL=https://download.bt.cn/cloudwaf/scripts/install\_waf\_slave.sh && if [ -f /usr/bin/curl ];then curl -sSO "\$URL" ;else wget -O install\_waf\_slave.sh "\$URL";fi;bash install\_waf\_slave.sh https://192.168.10.58:8381 wOFwsKhG21QRs3JWDsUn41VDrd7al15HV8ckus-DMyXF3xIRkla7rQfWzwbIZRX3Gm32Wtdfi5DbhiDwxl-qDV4KUyQ9RChxdRKldyvc\_hFgAq5pUtb7XtfxQ7F\_gvbeKoEB\_ifKDm\_if2Hzuxww CaFMdggmlnIUebQh4kV\_jpo 复制
- 安装被控完成后等待被控提交信息  
正在等待被控安装...
- 选择节点所属分组

取消 添加

使用SSH工具登录被控服务器，执行命令安装被控

```

System information as of Thu 11 Jan 2024 08:41:23 AM UTC

System load:                0.01
Usage of /:                  36.1% of 19.56GB
Memory usage:                32%
Swap usage:                  0%
Processes:                   150
Users logged in:             2
IPv4 address for ens18: 192.168.10.80
IPv6 address for ens18: fd54:4236:7cc6:0:3847:98ff:fe14:3663

* Strictly confined Kubernetes makes edge and IoT secure. Learn how MicroK8s
  just raised the bar for easy, resilient and secure K8s cluster deployment.

https://ubuntu.com/engage/secure-kubernetes-at-the-edge

136 updates can be installed immediately.
2 of these updates are security updates.
To see these additional updates run: apt list --upgradable

New release '22.04.3 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

*** System restart required ***
Last login: Thu Jan 11 08:40:55 2024 from ██████████
root@Slave-10-80:~#
root@Slave-10-80:~#

```

## 在线安装被控

推荐使用此安装方式

粘贴安装被控命令，按回车执行命令安装被控

- 注意需要ROOT权限执行命令

```

root@Slave-10-80:~#
root@Slave-10-80:~#
root@Slave-10-80:~# URL=https://download.bt.cn/cloudwaf/scripts/install_waf_slave.sh && if [ -f /usr/bin
/curl ];then curl -sSO "$URL" ;else wget -O install_waf_slave.sh "$URL";fi;bash install_waf_slave.sh htt
ps://192.168.10.58:8381 w0FwsKhG21QRs3JWDsUn41VDrd7al15HV8ckus-DMyXF3xlRkla7rQfWzwbIZRX3Gm32Wtdfi5DbhiDw
xI-qDV4KUyQ9RChxdRKldyvc_hH_CgmPpURRnfKV7grVhSx06Wuq0kQStQd-1jESbYxwJYvk5seDMXGvB6YdXFL5xyY

```

被控安装完成后显示以下信息

```
正在导入数据中,请耐心等待...
Restarting cloudwaf_nginx... done
Stopping ipfilter... done
Starting ipfilter... done
Stopping bt-cloudwaf... done
Starting bt-cloudwaf... done
Synchronizing state of btw.service with SysV service script with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable btw
Created symlink /etc/systemd/system/multi-user.target.wants/btw.service → /lib/systemd/system/btw.service.
Command may disrupt existing ssh connections. Proceed with operation (y|n)? Firewall is active and enabled on system startup
Default incoming policy changed to 'deny'
(be sure to update your rules accordingly)
Firewall reloaded
Time consumed: 3 Minute!
集群被控安装成功! 连接堡塔云WAF集群主控服务器地址为: https://192.168.10.58:8381
root@Slave-10-80:~#
```

安装完成后, 主控界面会显示被控的相关信息, 注意 **节点IP** 也就是网站域名A解析的IP (如果显示的信息不准确, 您可以进行修改为正确的信息)



添加新节点

A0anupSYx8JZu0Rb8T1DOKKGG9oRXMgTBQFWYfWwd9jmnfPgQTAUVc

**2 安装被控完成后等待被控提交信息**

✓ 安装被控成功

节点IP

地区

CPU  核

内存  GB

上行带宽  Mbps

系统

**3 选择节点所属分组**

负载分组

节点备注

取消
添加

集群设置 1 需求反馈

企业版
免费版
帮助
v1.0 更新 修复 重启

节点列表
DNS接管
负载均衡设置

添加节点

搜索节点名称

节点名称	状态	实时QPS	上行	下行	回源时间	负载	CPU	内存	操作
主控节点	● 在线	0	23.23 KB	22.73 KB	0ms	0.1 / 0.08 / 0.02	2.43%	55.19%	停用 修改 删除
192.168.10.80	● 在线	0	8.02 KB	18.41 KB	0ms	0.1 / 0.38 / 0.25	1.1%	51.48%	停用 修改 删除

20 / 页
<
1
>
共2条

被控添加已经完成。

## 离线安装被控

注意，此安装方式适用于服务器无法连接公网节点时的选择

- 离线安装时必须手动安装 docker，否则无法安装
- 离线安装前请确保您的服务器存在 tar gzip curl netstat ss docker 命令，可以使用此命令检查是否存在：

```
Packs=("curl" "tar" "gzip" "netstat" "ss" "docker" ); for pack in "${Packs[@]}";  
do command -v "$pack" >/dev/null 2>&1 || echo -e "\033[31mError: $pack 命令不存  
在\033[0m"; done
```

请根据您的系统架构下载安装文件，使用命令 `uname -m` 可以查看架构

x86\_64 架构：

- 离线安装脚本：[点击下载离线安装脚本](#)
- 下载镜像文件：[点击下载镜像 x86\\_64 架构文件](#)
- 下载cloudwaf程序文件：[点击下载cloudwaf程序 x86\\_64 架构文件](#)

aarch64 架构：

- 离线安装脚本：[点击下载离线安装脚本](#)
- 下载镜像 aarch64 架构文件：[点击下载镜像 aarch64 架构文件](#)
- 下载cloudwaf程序 aarch64 架构文件：[点击下载cloudwaf程序 aarch64 架构文件](#)

根据不同的系统架构下载文件后，使用Xftp、Winscp等工具上传到服务器中，将下载的文件放在相同的路径

## 修改被控安装命令

在 `主控IP` 方框处，输入您的 `主控IP`。我输入的是 192.168.10.58，然后点击 `获取命令`，最后点击 `复制` 复制安装被控命令

(请根据您的主控、被控 网络环境输入主控IP。被控必须可以连接到主控，否则将无法安装。)

宝塔云WAF 集群设置 2 需求反馈

节点列表 DNS接管 负载均衡设置

添加节点 剩余可用授权: 0

节点名称	状态	实时QPS	上行	下行	回源时
主控节点	● 在线	188	112.85 KB	183.84 KB	

添加新节点

- 复制节点安装命令，登录到被控服务器安装节点
 

主控IP  获取命令

```
URL=https://download.bt.cn/cloudwaf/scripts/install_waf_slave.sh && if [ -f /usr/bin/curl ];then curl -sSO "$URL" ;else wget -O install_waf_slave.sh "$URL";fi;bash install_waf_slave.sh https://192.168.10.58:8381 wOFwsKhG21QRs3JWDsUn41VDrd7al15HV8ckus-DMyXF3xIRkla7rQfWzwbIZRX3Gm32Wtdfi5DbhiDwxI-qDV4KUyQ9RChxdRKldyvc_hFgAq5pUtb7XtfxQ7F_gvbeKoEB_iFKDm_if2HzuxxwCaFMdggmInIUEbQh4kV_jpo
```
- 安装被控完成后等待被控提交信息
 

正在等待被控安装...
- 选择节点所属分组
 

请先完成步骤1

取消 添加

例如：

```
URL=https://download.bt.cn/cloudwaf/scripts/install_waf_slave.sh && if [ -f /usr/bin/curl ];then curl -sSO "$URL" ;else wget -O install_waf_slave.sh "$URL";fi;bash install_waf_slave.sh https://192.168.10.58:8381 wOFwsKhG21QRs3JWDsUn41VDrd7al15HV8ckus-DMyXF3xIRkla7rQfWzwbIZRX3Gm32Wtdfi5DbhiDwxI-qDV4KUyQ9RChxdRKldyvc_hFgAq5pUtb7XtfxQ7F_gvbeKoEB_iFKDm_if2HzuxxwCaFMdggmInIUEbQh4kV_jpo
```

将删除以下内容：

```
URL=https://download.bt.cn/cloudwaf/scripts/install_waf_slave.sh && if [ -f /usr/bin/curl ];then curl -sSO "$URL" ;else wget -O install_waf_slave.sh "$URL";fi;
```

即：

```
URL=https://download.bt.cn/cloudwaf/scripts/install_waf_slave.sh && if [ -f /usr/bin/curl ];then curl -sSO "$URL" ;else wget -O install_waf_slave.sh "$URL";fi; bash install_waf_slave.sh https://192.168.10.58:8381 wOFwsKhG21QRs3JWDsUn41VDrd7al15HV8ckus-DMYXF3xIRkla7rQfWzwbIZRX3Gm32Wtdfi5DbhiDwxI-qDV4KUyQ9RChxdRKldyvc_hFgAq5pUtb7XtfxQ7F_gvbeKoEB_iFKDm_if2HzuxxwCaFMdggmlnIUEbQh4kV_jpo
```

再到命令后，添加 **offline** 离线安装标识，最终的安装被控命令：

```
bash install_waf_slave.sh https://192.168.10.58:8381 wOFwsKhG21QRs3JWDsUn41VDrd7al15HV8ckus-DMYXF3xIRkla7rQfWzwbIZRX3Gm32Wtdfi5DbhiDwxI-qDV4KUyQ9RChxdRKldyvc_hFgAq5pUtb7XtfxQ7F_gvbeKoEB_iFKDm_if2HzuxxwCaFMdggmlnIUEbQh4kV_jpo offline
```

请以您复制的安装命令修改为准，以上为示例  
复制修改之后的命令到被控服务器上安装。

在 被 控服务器上执行安装命令离线安装：

注意需要ROOT权限执行命令

安装完成后，登录步骤与在线相同 示例为：x86\_64 架构

```
root@Slave-10-80:~/11#
root@Slave-10-80:~/11# ls -al
total 231684
drwxr-xr-x 2 root root    4096 Jan 12 07:35 .
drwx----- 9 root root    4096 Jan 12 07:29 ..
-rw-r--r-- 1 root root 192053434 Jul  7 2023 btwaf_mysql_openresty-latest.tar.gz
-rw-r--r-- 1 root root    91238 Jan 11 07:52 install_waf_slave.sh
-rw-r--r-- 1 root root  45077085 Jan 12 07:05 waf-cluster-latest.tar.gz
root@Slave-10-80:~/11#
root@Slave-10-80:~/11#
root@Slave-10-80:~/11# bash install_waf_slave.sh https://192.168.10.58:8381 wOFwsKhG21QRs3JWDsUn41VDrd7al15HV8ckus-DMYXF3xIRkla7rQfWzwbIZRX3Gm32Wtdfi5DbhiDwxI-qDV4KUyQ9RChxdRKldyvc_hFgAq5pUtb7XtfxQ7F_gvbeKoEB_iFKDm_if2HzuxxwCaFMdggmlnIUEbQh4kV_jpo offline
```

- 被控安装方式

- 在主控界面获取被控安装命令：
- 在线安装被控

## 安装被控

- 离线安装被控
- 请根据您的系统架构下载安装文件，使用命令 `uname -m` 可以查看架构
  - 修改被控安装命令

# 更新日志

---

- [堡塔云WAF集群版 更新日志](#)
  - [2024-01-15 V1.1 正式版本](#)
  - [2024-01-12 V1.0 正式版本](#)

## 堡塔云WAF集群版 更新日志

### 2024-01-15 V1.1 正式版本

---

【修复】云WAF一处SQL注入BUG

### 2024-01-12 V1.0 正式版本

---

发布堡塔云WAF集群版

# 恶意IP共享计划

## 堡塔恶意IP共享计划

本文档更新时间为：2023年10月31日

亲爱的堡塔用户，您好！

为了向用户提供简单好用的产品，一直是堡塔公司追求的目标。堡塔恶意IP共享计划允许全球的堡塔用户共享恶意攻击IP，帮助其他用户识别攻击风险，实现自动拦截，提升服务器安全性，堡塔在此诚挚邀请您加入我们的堡塔恶意IP共享计划，请您仔细查阅以下声明。

您同意，当您加入堡塔恶意IP共享计划时，已经仔细阅读并完全同意本计划（未成年人应由监护人同意相关条款）。堡塔在此提示您，随产品发展，本声明有不定期更改之可能，如有更改，将会在产品或相关页面显着位置予以发布公告并明示用户。如果您不同意加入该计划或不同意更改内容，您有权随时退出计划（详见“加入和退出计划”）。

### 一、信息的收集

为了向您提供更好的产品和/或服务及保障您的账号安全，经您授权参与本计划，用户仅向堡塔发送基于以下目的的数据：

网络诊断和使用功能：

- 设备属性信息，包括国家/地区、系统版本、设备型号、系统信息、服务器IP、攻击者IP；
- 设备及其相关组件使用日志，包括系统和设备出现异常后相关日志信息。

如果不提供上述信息，将不影响产品功能的使用，但无法使用堡塔恶意IP库。

收集恶意IP相关信息时，我们尊重您的隐私，更多相关信息请查看我们的[隐私政策](#)。

### 二、信息的使用

堡塔在此承诺，堡塔严格遵守国家相关法律法规。堡塔将对收集的信息和内容严格保密，仅为提高产品质量并改善产品服务而使用上述信息，不会提供给任何与该目的无关的第三方公司。若您不提供这类信息，您需要手动更新IP库，无法动态实时更新。

关于我们如何使用您的信息，下面提供了更多详细示例：

- 提升防火墙拦截恶意攻击的准确度，检测攻击类型、攻击次数。
- 储存并维护与您相关的信息，用于我们的业务运营（例如业务统计）或履行法律义务。
- 改善用户体验，允许堡塔分析用户如何使用设备和系统服务的数据，以改善用户体验，例如发送崩溃报告。

### 三、我们如何存储并保护个人信息

堡塔采用普遍接受的行业安全标准，采取加密措施保护用户的个人信息和数据，以保证您的信息在未经授权的情况下不会被访问、使用或披露。所收集的相关数据在中国地区数据中心存储。

在技术方面，堡塔使用防病毒软件，加密保护、监控系统，增强堡塔数据中心的攻击防护。在制度方面，通过对堡塔员工进行安全与隐私保护知识培训，确保员工了解数据保护的重要性。但基于网络的固有缺陷及运行风险，堡塔并不能保证您的信息绝对安全。

## 四、加入和退出计划

---

用户可以根据自身意愿，在堡塔云WAF产品的\*\*"设置" - "加入恶意IP共享计划"项目中，自由选择开启或关闭。

如果用户选择开启，即表示用户选择参与堡塔恶意IP共享计划；如果用户选择关闭，即可退出恶意IP共享计划。