

# 宙斯盾安全防护

## 操作指南

## 产品文档



腾讯云

**【版权声明】**

©2013-2020 腾讯云版权所有

本文档（含所有文字、数据、图片等内容）完整的著作权归腾讯云计算（北京）有限责任公司单独所有，未经腾讯云事先明确书面许可，任何主体不得以任何形式复制、修改、使用、抄袭、传播本文档全部或部分内容。前述行为构成对腾讯云著作权的侵犯，腾讯云将依法采取措施追究法律责任。

**【商标声明】**

及其它腾讯云服务相关的商标均为腾讯云计算（北京）有限责任公司及其关联公司所有。本文档涉及的第三方主体的商标，依法由权利人所有。未经腾讯云及有关权利人书面许可，任何主体不得以任何方式对前述商标进行使用、复制、修改、传播、抄录等行为，否则将构成对腾讯云及有关权利人商标权的侵犯，腾讯云将依法采取措施追究法律责任。

**【服务声明】**

本文档意在向您介绍腾讯云全部或部分产品、服务的当时的相关概况，部分产品、服务的内容可能不时有所调整。您所购买的腾讯云产品、服务的种类、服务标准等应由您与腾讯云之间的商业合同约定，除非双方另有约定，否则，腾讯云对本文档内容不做任何明示或默示的承诺或保证。

**【联系我们】**

我们致力于为您提供个性化的售前购买咨询服务，及相应的技术售后服务，任何问题请联系 4009100100。

## 文档目录

### 操作指南

开启水印防护

通过 TOA 方案获取客户端 IP 地址

配置 HTTP CC 防护高级策略

配置 DDoS 防护高级安全策略

防护域名绑定高防 IP

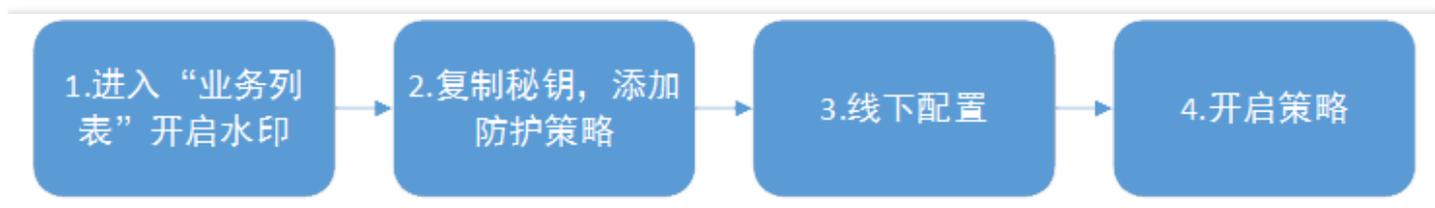
# 操作指南

## 开启水印防护

最近更新时间：2019-09-10 15:31:28

客户可以通过接入水印防护，高效全面防护4层 CC 攻击，如模拟业务报文攻击和重放攻击等。水印防护通过在业务端和宙斯盾防护系统端共享水印算法和密钥，使客户端每个发出的报文都嵌入了水印特征。而攻击报文却无水印特征，防护系统将甄别出攻击报文并将其丢弃。更详细的配置说明，详情请参见 [自定义高级安全策略](#)。

### 流程图



### 开启流程

#### 1. \*\* 进入“业务列表”开启水印\*\*

用户进入 [宙斯盾高防控制台](#)，在左侧目录中单击【业务域名列表】，在已经创建的对应项目列，单击【开启水印】。

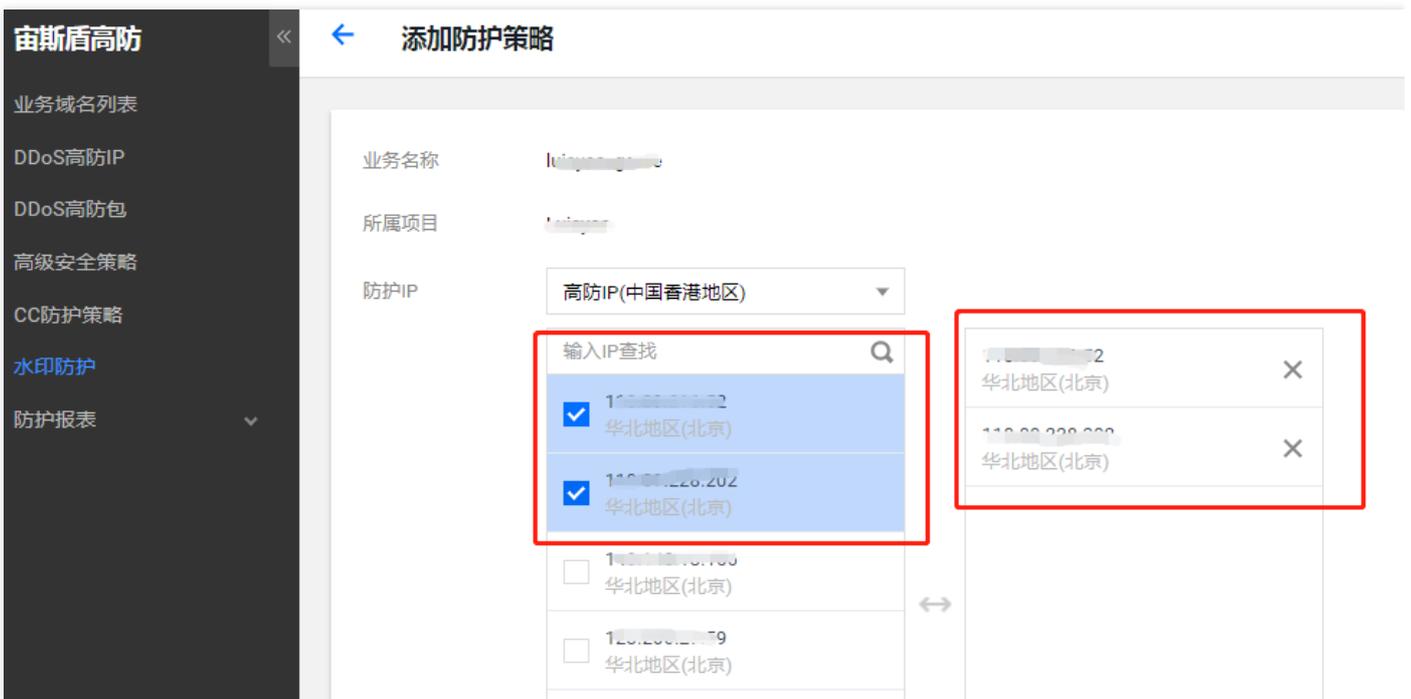


#### 2. 复制密钥

a. 开启水印成功后，在“水印功能开启成功”的弹窗中选择“复制密钥”，单击【添加防护策略】。



b. 进入“添加防护策略”页面，选择“防护 IP”。



c. 添加好 TCP 协议防护端口、UDP 协议防护端口、白名单，单击【确认添加】。



### 3. 线下配置

在“水印功能开启成功”弹窗中，单击【客户端接入文件】下载，完成客户端和服务端的接入。

### 4. 开启策略

a. 用户创建策略成功后，在【水印防护】下，单击【增加策略】进行修改，单击【启用】策略。



b. 等待几秒钟，防护状态显示为“防护生效”，水印开启成功。

The screenshot shows the 'Watermark Protection' (水印防护) configuration page in the Tencent Cloud console. The left sidebar contains navigation options: 宙斯盾高防, 业务域名列表, DDoS高防IP, DDoS高防包, 高级安全策略, CC防护策略, 水印防护, and 防护报表. The main content area is titled '水印防护' and includes a search bar for IP addresses or ports. A table lists the protection status for various services. The 'elearn-test' service is highlighted with a red box around its '防护状态' (Protection Status), which is '防护生效' (Protection Effective). The table also shows the protection IP (200.0.0.0/0), TCP and UDP ports (80, 8080, 25), and the activation time (2018/08/09 15:08:51). Action buttons for '策略详情', '停用', '删除', and '增加策略' are visible for the selected service.

业务名称	防护IP	TCP防护端口	UDP防护端口	防护状态	接入时间	操作
elearn-test	200.0.0.0/0	80, 8080	25	防护生效	2018/08/09 15:08:51	<a href="#">策略详情</a> <a href="#">停用</a> <a href="#">删除</a> <a href="#">增加策略</a>

共1项 每页显示行 20 1/1

# 通过 TOA 方案获取客户端 IP 地址

最近更新时间：2019-09-10 15:32:59

业务请求经过高防 IP 的 4 层转发后，业务服务器端接收到报文后，其看到的源 IP 地址是高防 IP 的出口 IP 地址。为了让服务器端能够获取到用户端实际的 IP 地址，可以使用如下 TOA 的方案。在业务服务的 Linux 服务器上，安装对应的 TOA 内核包，并重启服务器后。业务侧就可以获取到用户端实际的 IP 地址。

## TOA 原理

高防转发后，数据包同时会做 SNAT 和 DNAT，数据包的源地址和目标地址均修改。

TCP 协议下，为了将客户端 IP 传给服务器，会将客户端的 IP，port 在转发时放入了自定义的 tcp option 字段。

```
#define TCPOPT_ADDR 200
#define TCPOLEN_ADDR 8 /* |opcode|size|ip+port| = 1 + 1 + 6 */

/*
 *insert client ip in tcp option, now only support IPV4,
 *must be 4 bytes alignment.
 */
struct ip_vs_tcpo_addr {
    __u8 opcode;
    __u8 opsize;
    __u16 port;
    __u32 addr;
};
```

Linux 内核在监听套接字收到三次握手的 ACK 包之后，会从 SYN\_RECV 状态进入到 TCP\_ESTABLISHED 状态。这时内核会调用 tcp\_v4\_syn\_recv\_sock 函数。Hook 函数 tcp\_v4\_syn\_recv\_sock\_toa 首先调用原有的 tcp\_v4\_syn\_recv\_sock 函数，然后调用 get\_toa\_data 函数从 TCP OPTION 中提取出 TOA OPTION，并存储在 sk\_user\_data 字段中。

然后用 inet\_getname\_toa hook inet\_getname，在获取源 IP 地址和端口时，首先调用原来的 inet\_getname，然后判断 sk\_user\_data 是否为空，如果有数据从其中提取真实的 IP 和 port，替换 inet\_getname 的返回。

客户端程序在用户态调用 getpeername，返回的 IP 和 port 即为客户端的原始 IP。

## 内核包安装步骤

### Centos 6.x/7.x

## 安装步骤

### 1. 下载安装包

- (1) [Centos 6.x 下载](#)
- (2) [Centos 7.x 下载](#)

### 2. 安装包文件

```
rpm -hiv kernel-2.6.32-220.23.1.el6.toa.x86_64.rpm --force
```

### 3. 安装完成之后重启主机

```
reboot
```

### 4. 执行命令检查 toa 模块是否加载成功

```
lsmod | grep toa
```

### 5. 没有加载的话手工开启

```
modprobe toa
```

### 6. 可用下面的命令开启自动加载 toa 模块

```
echo "modprobe toa" >> /etc/rc.d/rc.local
```

## Ubuntu 16.04

下载安装包：

- (1) [内核包下载](#)
- (2) [内核 header 包下载](#)

安装步骤：

```
dpkg -i linux-image-4.4.87.toa_1.0_amd64.deb
```

Headers 包可不装，如需要做相关开发则安装。

安装完成之后重启主机，然后 `lsmod | grep toa` 检查 toa 模块是否加载 没有加载的话 `modprobe toa` 开启。

可用下面的命令开启加载 toa 模块

```
echo "modprobe toa" >> /etc/rc.d/rc.local
```

## Debian 8

(1) [内核包下载](#)

(2) [内核 header 包下载](#)

安装方法与 Ubuntu 相同。

请根据业务服务器 Linux 操作系统的类型和版本下载对应的内核包，按如下步骤操作。如果没有和用户操作系统一致的内核包，用户还可以参考下面 TOA 源代码安装指引操作。

# TOA 源代码内核安装指引

## 源码安装

1. 下载打好 [toa 补丁](#) 的源码包，单击 toa 补丁即可下载安装包。
2. 解压。
3. 编辑 .config，将 CONFIG\_IPV6=M 改成 CONFIG\_IPV6=y。
4. 如果需要加上一些自定义说明，可以编辑 Makefile。
5. make -jn (n 为线程数)。
6. make modules\_install。
7. make install。
8. 修改 /boot/grub/menu.lst 将 default 改为新安装的内核 (title 顺序从 0 开始)。
9. Reboot 重启后即为 toa 内核。
0. lsmod | grep toa 检查 toa 模块是否加载 没有加载的话 modprobe toa 开启。

## 内核包制作

可自己制作 rpm 包，也可由我们提供。

1. 安装 kernel-2.6.32-220.23.1.el6.src.rpm

```
rpm -hiv kernel-2.6.32-220.23.1.el6.src.rpm
```

2. 生成内核源码目录

```
rpmbuild -bp ~/rpmbuild/SPECS/kernel.spec
```

### 3. 复制一份源码目录

```
cd ~/rpmbuild/BUILD/kernel-2.6.32-220.23.1.el6/ cp -a linux-2.6.32-220.23.1.el6.x86_64/ linux-2.6.32-220.23.1.el6.x86_64_new
```

### 4. 在复制出来的源码目录中打toa 补丁

```
cd ~/rpmbuild/BUILD/kernel-2.6.32-220.23.1.el6/linux-2.6.32-220.23.1.el6.x86_64_new/  
patch -p1 < /usr/local/src/linux-2.6.32-220.23.1.el6.x86_64.rs/toa-2.6.32-220.23.1.el6.patch
```

### 5. 编辑.config 并拷贝到 SOURCE 目录

```
sed -i 's/CONFIG_IPV6=m/CONFIG_IPV6=y/g' .config  
echo -e '\n# toa\nCONFIG_TOA=m' >> .config  
cp .config ~/rpmbuild/SOURCES/config-x86_64-generic
```

### 6. 删除原始源码中的.config

```
cd ~/rpmbuild/BUILD/kernel-2.6.32-220.23.1.el6/linux-2.6.32-220.23.1.el6.x86_64  
rm -rf .config
```

### 7. 生成最终 patch

```
cd ~/rpmbuild/BUILD/kernel-2.6.32-220.23.1.el6/  
diff -uNr linux-2.6.32-220.23.1.el6.x86_64 linux-2.6.32-220.23.1.el6.x86_64_new/ >  
~/rpmbuild/SOURCES/toa.patch
```

### 8. 编辑 kernel.spec

```
vim ~/rpmbuild/SPECS/kernel.spec
```

在ApplyOptionPath 下添加如下两行（还可修改 buildid 等自定义内核包名）

```
Patch999999: toa.patch
```

```
ApplyOptionalPatch toa.patch
```

## 9. 制作 rpm 包

```
rpmbuild -bb --with baseonly --without kabichk --with firmware --without debuginfo --target=x86_64 ~/rpmbuild/SPECS/kernel.spec
```

## 10. 安装内核 rpm 包

```
rpm -hiv kernel-xxxx.rpm --force
```

重启，加载 toa 模块

# 配置 HTTP CC 防护高级策略

最近更新时间：2019-09-10 15:34:59

宙斯盾安全防护（Aegis Anti-DDoS）提供 HTTP CC 高级防护策略，CC 防护策略当设置 HTTP 请求数超过设定的 QPS 值时，才会触发 CC 防护。更详细的配置说明，详情请参见 [自定义高级安全策略](#)。

## 添加 CC 防护策略

1. 用户进入 [宙斯盾高防控制台](#)，在左侧目录中，单击【HTTP CC 防护高级策略】，在“HTTP CC 防护高级策略”下，单击【添加新策略】。添加成功后，在“操作”列下单击【配置】进入策略配置页面。



2. 根据业务特点和防护需求配置 HTTP QPS 请求阈值、URL 白名单、IP 黑白名单、CC 自定义防护模式等策略。单击保存即添加策略成功。

CC自定义防护模式  关闭  开启

匹配模式

匹配规则	执行动作	操作
User Agent 包含 baidu	人机验证	<a href="#">编辑</a> <a href="#">删除</a>
Host 包含 www.sina.com	阻断	<a href="#">编辑</a> <a href="#">删除</a>
CGI 不包含 xxgame	人机验证	<a href="#">编辑</a> <a href="#">删除</a>
<a href="#">添加策略</a>		

限速模式

源IP全局限速① 每个源IP访问速率 (次/分钟)

域名①	每个源IP访问速率 (次/分钟)	操作
<input type="text" value="www.test.com"/>	<input type="text" value="10"/>	<a href="#">删除</a>
<a href="#">添加策略</a>		

[确定](#) [取消](#)

## CC 防护策略直接绑定防护 IP

1. 单击【HTTP CC 防护高级策略】，在“HTTP CC 防护高级策略”下单击“策略 ID”。

HTTP CC防护高级策略 全部项目 产品帮助

[添加新策略](#)

策略ID/名称	绑定IP数量	所属项目	创建时间	操作
	2	默认项目	2018-03-02 18:29:49	<a href="#">配置</a> <a href="#">复制</a> <a href="#">删除</a> <a href="#">绑定IP</a>

2. 单击【绑定 IP 列表】，单击【添加 IP】。



## DDoS 高防 IP 绑定 CC 防护策略

1. 单击【DDoS 高防 IP】，在“DDoS 高防 IP”下，选择“高防 IP”，进入“DDoS 高防 IP”详情页。



2. 单击“高级配置信息”。单击【绑定】，选择好 CC 防护策略，单击【确认】。



## 给 DDoS 高防包下的防护 IP 配置 CC 防护策略

1. 单击【DDoS 高防包】，在“DDoS 高防包”下，选择“高防包 ID”，进入“DDoS 高防包”详情页。



2. 单击【防护 IP 列表】，勾选需要配置的 IP，单击“配置 CC 防护策略”。

DDoS高防包详情 ( )

基本信息 **防护IP列表**

防护IP配置

最多可添加5个IP，已添加2个IP。

添加防护IP 绑定DDoS防护高级策略 **绑定HTTP CC防护高级策略** 绑定到业务 移除IP

<input type="checkbox"/>	资源ID/名称	IP地址	所属项目	资源类型	DDoS防护高级策略	HTTP CC防护高级策	防护状态	绑定业务	最近_①	操作
<input checked="" type="checkbox"/>	lb- 2c						正常			<a href="#">解绑高级安全策略</a> <a href="#">解绑CC防护策略</a> <a href="#">绑定业务</a>

# 配置 DDoS 防护高级安全策略

最近更新时间：2019-12-10 10:07:37

宙斯盾安全防护（Aegis Anti-DDoS）提供 DDoS 高级安全防护策略。用户可针对业务平台的自身需求配置，绑定到高防 IP、高防包防护的 IP 上，通过禁用协议、禁用端口、IP 黑白名单、报文特征过滤策略、空连接防护等操作，为业务平台提供针对性防护。更详细的配置说明，详情请参见 [自定义高级安全策略](#)。

## 添加高级安全策略

1. 用户进入 [宙斯盾高防控制台](#)，在左侧目录中，单击【DDoS 防护高级策略】，在“DDoS 防护高级策略下”，单击【添加新策略】。添加成功后，在“操作”列下单击【配置】进入策略配置页面。



2. 选择需要配置的禁用协议跟端口，设置 IP 黑白名单，报文特征过滤，可选择性开启拒绝境外流量、空连接防护。单击【确定】即添加策略成功。

拒绝海外流量 <sup>①</sup>  关闭  开启

空链接防护  关闭  开启

**IP黑白名单**

IP白名单 [增加](#)

IP黑名单 [增加](#)

**报文特征过滤策略**

协议	开始端 <sup>①</sup>	结束端 <sup>①</sup>	最小包长 <sup>①</sup>	最大包长 <sup>①</sup>	检测载荷	偏移量 <sup>①</sup>	检查深度 <sup>①</sup>	是否包括	字符串	策略	操作
TCP	80	80	1000	1500	检测...	0	150	包含	GET	丢弃	删除
TCP	80	80	1000	1500	检测...	0	1500	包含	Host	丢弃	删除

[增加](#)

[确定](#) [取消](#)

## 高级安全策略直接绑定防护 IP

1. 单击【DDoS 防护高级策略】，在“DDos 防护高级策略下”，单击“策略 ID”。

**DDoS防护高级策略** 全部项目 产品帮助

[添加新策略](#)

策略ID/名称	绑定IP数量	所属项目	创建时间	操作
	4	默认项目	2018-03-02 18:26:08	<a href="#">配置</a> <a href="#">复制</a> <a href="#">删除</a> <a href="#">绑定IP</a>

2. 在“DDoS 防护高级策略下”，单击【绑定IP列表】，单击【添加IP】。



## DDoS 高防 IP 绑定高级安全策略

1. 单击【DDoS 高防 IP】，在“DDoS 高防 IP”下，单击“高防 IP”。



2. 在“DDoS 高防 IP 详情”页下单击【高级配置】。单击【绑定】，在“配置 DDoS 防护高级策略”弹窗中，选择

好“DDoS 防护高级安全策略”，单击【确认】。



## 给 DDoS 高防包下的防护 IP 配置高级安全策略

1. 单击【DDoS 高防包】，在“DDoS 高防包”下，单击高防包 ID。



2. 在“DDoS 高防包详情”页下单击【防护 IP 列表】，勾选需要配置的 IP，单击“配置高级安全策略”。



# 防护域名绑定高防 IP

最近更新时间：2020-05-27 16:07:35

登录 [宙斯盾高防产品控制台](#)，在左侧目录中，选择“业务域名列表”，在右侧页面中，单击“创建业务和域名”创建业务，并自动生成防护域名。用户可通过将业务域名 CNAME 到防护域名接入高防。

## 流程图



## 防护域名绑定高防 IP 的流程

### 1. 创建业务

a. 单击【业务域名列表】，在“业务域名列表”下，单击【创建业务和域名】。



b. 填写好相关信息，单击【创建】，创建成功后立即在“业务域名列表”生成业务和免费的防护域名。

←

## 创建业务和域名

**创建业务和域名**

所属项目 默认项目

业务名称 请输入业务名称

联系人姓名 请输入联系人姓名

手机号码 请输入手机号码

开发平台  PC客户端  移动端  电视端  主机

细分品类 请选择细分品类

创建

## 2. 添加高防 IP

a. 在业务域名列表管理页下，单击“添加 IP”，跳转到业务详情页。

### 业务域名列表

全部项目

创建业务和域名

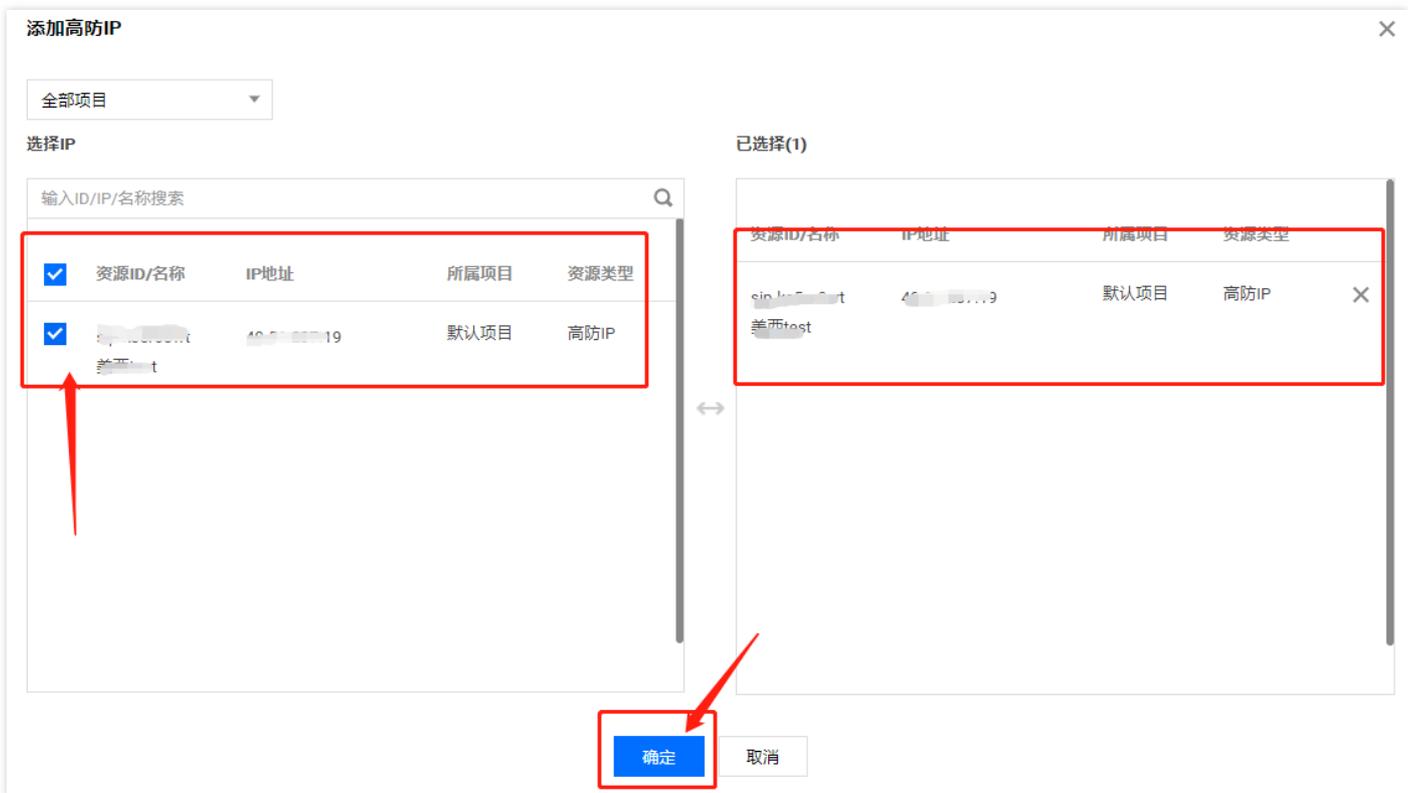
输入业务名称搜索 Q

业务名称	防护域名	高防IP资源	DNS解析状...	BGP优先状...	业务水印防...	创建时间	操作
test01	www.qq.com	<span style="border: 1px solid red; padding: 2px;">添加IP</span>	-	已启用	已启用	2018-07-19 15:14:36	<a href="#">配置</a> <a href="#">删除</a> <a href="#">关闭水印</a>

b. 在业务详情页下的 IP 资源和解析设置单击“添加 IP”。



c. 勾选高防 IP，单击【确定】。



### 3. 开启域名解析

添加高防 IP 成功后，开启“域名解析”。防护域名提供智能解析，即根据用户来源 IP 解析到对应线路的 IP。如电信用户会解析到电信的高防 IP，联通用户会解析到联通的高防 IP 等。若某一线路的高防 IP 因攻击超峰被封堵，则会智能解析到其他可用的高防 IP。

BGP 线路优先开关开启时，若有绑定 BGP 线路 IP，则防护域名会优先调度所有业务请求解析到 BGP 的 IP 地址。（其他开启解析开关的三网高防 IP 处于备用状态）。若发生大流量攻击导致 BGP 高防 IP 被封堵，则系统会智能调度业务请求到开启域名解析开关的三网高防 IP，以提供高带宽防护能力。若 BGP 高防 IP 解除封堵，则系

统会恢复将所有业务请求调度到 BGP 高防 IP。

**防护域名解析设置**

域名: [redacted]

TTL值: 10分钟 [调整](#)

BGP线路优先

IP资源和解析设置 [添加IP](#)

资源ID	IP地址	线路	区域	运行状态	域名解析	操作
[redacted]	[redacted] 默认	联通	华东	运行中	<input checked="" type="checkbox"/>	<a href="#">解除绑定</a>

#### 4. 主域名 CNAME 到防护域名

线路解析开启后，业务主域名可通过 CNAME 到防护域名，智能解析到高防 IP。

← **werekf.com** 全部项目

域名信息 **域名解析**

**业务域名**

注意：在中国大陆地区开展网站服务，请先将域名进行备案，否则将无法访问。[开始备案](#)  
需要修改域名DNS为：[fsgw...](#) [fsgw...](#) [一键修改](#)  
修改DNS服务器需要最长72个小时的全球生效时间，请耐心等待。  
[遇到问题？查看FAQ文档](#)

[记录管理](#) | [负载均衡](#) | [解析量统计](#) | [域名设置](#) | [自定义线路](#) | [线路分组](#)

[添加记录](#) [新手快速添加](#) [暂停](#) [开启](#) [删除](#) [分配至项目](#)

<input type="checkbox"/>	主机记录	记录类型	线路类型	记录值	优先级	TTL (秒)	最后操作时间	操作
<input type="checkbox"/>	@	CNAME	默认	<a href="#">b2f...</a>	-	600	2018-07-30 19:40:05	<a href="#">修改</a> <a href="#">暂停</a> <a href="#">删除</a>
<input type="checkbox"/>	*	CNAME	默认	<a href="#">b2f...</a>	-	600	-	<a href="#">保存</a>

用户验证，例如在本地用 ping 或者 nslookup 方式检查是否域名能够解析到高防 IP。

