

## 目录

目录	1
高防IP管理	2
目录	2
开启(关闭)高防	2
删除高防	2
查看防护数据	2
操作步骤	2
名词解释	2
七层配置	3
目录	3
添加域名记录	3
健康检查配置	3
源站配置	4
四层配置	4
目录	4
添加转发设置	4
健康检查配置	5
源站配置	6
CC防护设置	6
目录	6
高防级别	6
开启(关闭)CC防护	6
域名记录级别	7
开启(关闭)CC防护	7
添加自定义CC防护规则	7
修改CC防护设置	8

## 高防IP管理

本文档简要介绍了高防IP实例的开启、关闭、删除操作过程。

### 目录

[开启\(关闭\)高防](#)

[删除高防](#)

### 开启(关闭)高防

选择要开启的高防IP实例，点击上侧的**开启**按钮，在弹出的确认框中单击**确定**。



防护状态中显示高防为已开启状态，操作完成。

关闭高防同理

[返回目录](#)

### 删除高防

选择要关闭的高防IP实例，点击上侧的**删除**按钮，在弹出的确认框中单击**确定**。



注意：只有已过期的实例才可以删除

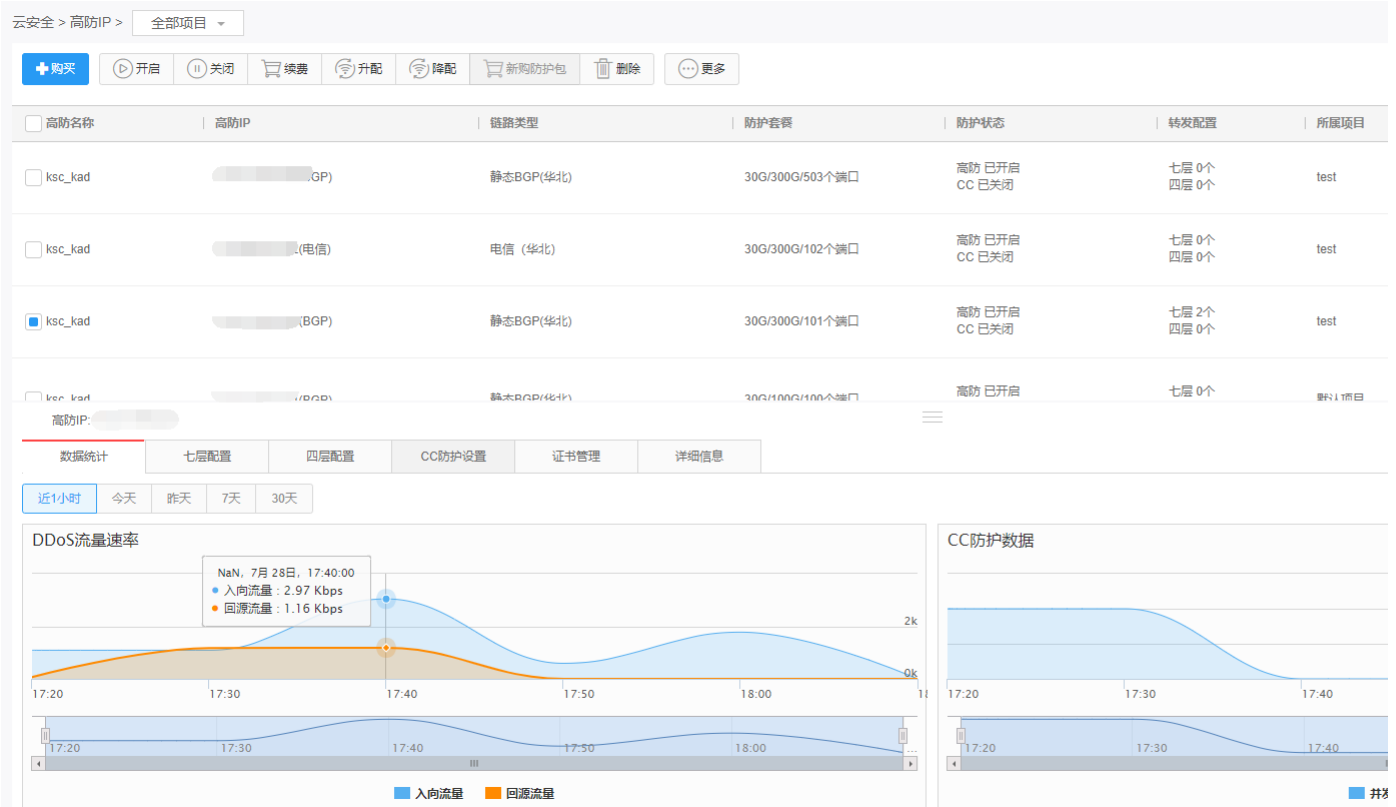
[返回目录](#)

## 查看防护数据

本文档介绍了高防IP的防护数据的查看方式。

### 操作步骤

1. 选择一个高防IP实例。
2. 在底部滑出面板的**数据统计**中查看高防的防护数据。



### 名词解释

**入向流量**：经过高防清洗设备、被识别为恶意攻击的流量和正常的流量 **回源流量**：从高防清洗设备回到用户源站的下行流量 **并发连接数**：外界对域名发起的连接总数

## 七层配置

本文档介绍了网站业务接入的七层配置方式。

### 目录

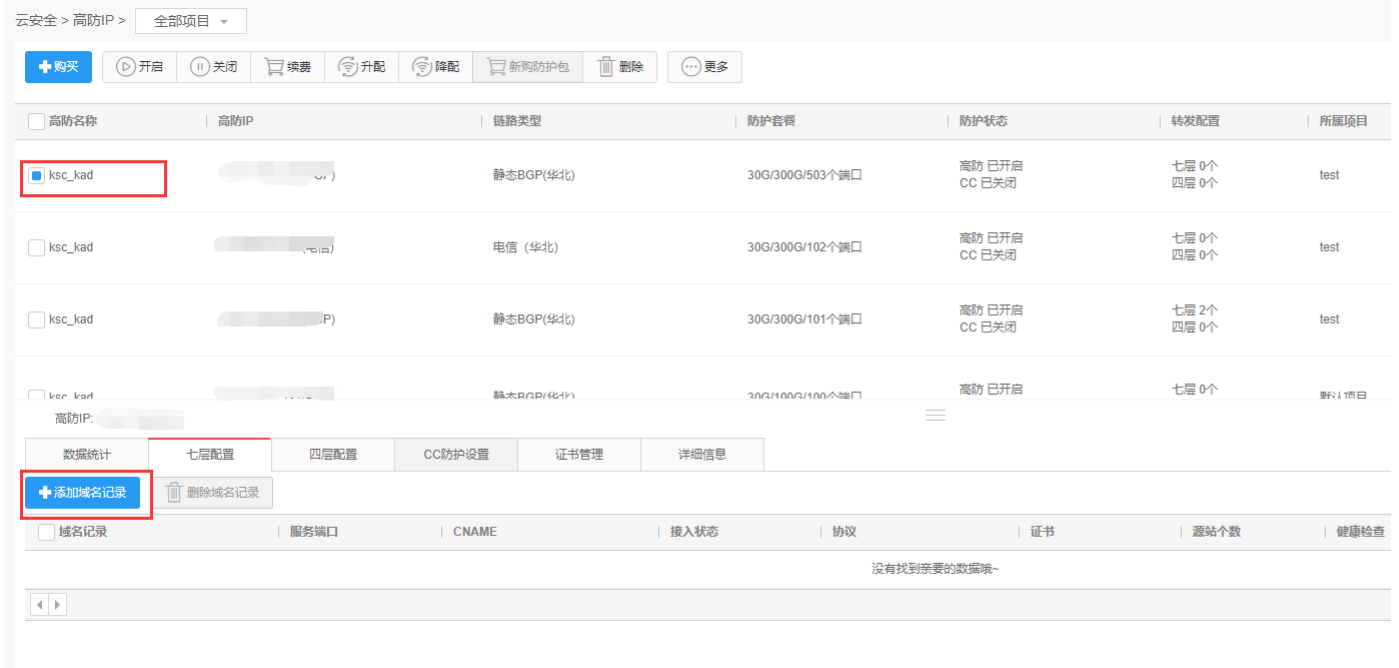
[添加域名记录](#)

[健康检查配置](#)

[源站配置](#)（编辑源站主机的信息）

### 添加域名记录

1. 选择一个高防IP实例。
2. 在底部滑出面板中选择**七层配置**页签，并点击**添加域名记录**。



3. 在添加域名记录的对话框中，正确填写高防服务端口、域名记录、协议等参数。当**健康检查**开启时，需填写健康检查参数。

#### 添加域名记录

\*高防服务端口:

\*域名记录:

\*协议:

http协议不能配置443的高防服务端口, https协议不能配置80的高防服务端口和源站端口

\*证书: --

\*源站数据中心:

\*源站IP:

\*端口:

健康检查:

健康检查间隔(s):  秒 ?

健康阈值(次):  次 ?

不健康阈值(次):  次 ?

\*HTTP请求链接:

域名:

健康检查IP: 27.155.93.64/27  
59.153.74.128/25  
120.221.146.0/24  
140.249.26.0/24  
119.167.167.0/24

4. 点击**添加**，域名记录配置成功。

[返回目录](#)

### 健康检查配置

1. 在域名记录中，点击**健康检查配置**。
2. 在**健康检查配置**弹窗中可设置健康检查开启或关闭，并对健康检查参数进行配置。

## 健康检查配置



域名记录: [REDACTED]

高防服务端口: 80

健康检查:

健康检查间隔(s):  秒 ?

健康阈值(次):  次 ?

不健康阈值(次):  次 ?

HTTP请求链接:

域名: [REDACTED]

健康检查IP: 27.155.93.64/27  
59.153.74.128/25  
120.221.146.0/24  
140.249.26.0/24  
119.167.167.0/24

3. 点击**确定**，完成健康检查配置。

[返回目录](#)

## 源站配置

1. 在域名记录中，点击**源站配置**。

高防IP: [REDACTED] ≡

数据统计 | **七层配置** | 四层配置 | CC防护设置 | 证书管理 | 详细信息

<input type="checkbox"/> 域名记录	服务端口	CNAME	接入状态	协议	证书	源站个数	健康检查
<input checked="" type="checkbox"/> test.ksyun.com	80	[REDACTED].com	未接入	HTTP	-	1	开启

2. 在**源站配置**弹窗中，可对已有配置进行修改，点击**添加源站配置**，可新增一条配置信息。

3. 点击**确定**，配置成功。

[返回目录](#)

## 四层配置

本文档介绍了四层业务接入的配置方式。

## 目录

[添加转发设置](#)

[健康检查配置](#)

[源站配置](#)（编辑源站主机的信息）

## 添加转发设置

1. 选择一个高防IP实例。
2. 在底部滑出面板中选择**四层配置**页签，并单击**添加转发设置**按钮。

云安全 > 高防IP > 全部项目

高防名称	高防IP	链路类型	防护套餐	防护状态	转发配置	所属项目
<input type="checkbox"/> ksc_kad	(BGP)	静态BGP(华北)	30G/300G/503个端口	高防 已开启 CC 已关闭	七层 0个 四层 0个	test
<input type="checkbox"/> ksc_kad	(电信)	电信 (华北)	30G/300G/102个端口	高防 已开启 CC 已关闭	七层 0个 四层 0个	test
<input checked="" type="checkbox"/> ksc_kad	(BGP)	静态BGP(华北)	30G/300G/101个端口	高防 已开启 CC 已关闭	七层 2个 四层 0个	test
<input type="checkbox"/> ksc_kad	(BGP)	静态BGP(华北)	30G/300G/100个端口	高防 已开启	七层 0个	默认项目

高防IP: [ ]

CNAME: [ ] .com

转发协议	服务端口	CNAME	真实服务器个数	健康检查
<input type="checkbox"/>				

没有找到您要的数据哦~

3. 在添加转发设置的对话框中，选择协议，正确填写服务端口等参数，当**健康检查**开启时，需填写健康检查参数。

添加转发设置

\*协议:

\*服务端口:

\*源站数据中心:

\*真实服务器IP:

\*真实服务器端口:

健康检查:

健康检查间隔(s):  秒 ?

健康阈值(次):  次 ?

不健康阈值(次):  次 ?

健康检查IP: 27.155.93.64/27  
59.153.74.128/25  
120.221.146.0/24  
140.249.26.0/24  
119.167.167.0/24

4. 单击**添加**，转发设置配置成功。

[返回目录](#)

### 健康检查配置

1. 在域名记录中，单击**健康检查配置**。
2. 在弹窗中可设置健康检查开启或关闭，并对健康检查参数进行配置。

高防IP: [ ]

CNAME: [ ] .com

转发协议	服务端口	CNAME	真实服务器个数	健康检查
<input type="checkbox"/> TCP	111	[ ] .com	1	开启

3. 点击**确定**，健康检查配置成功。

### 健康检查配置

高防服务端口: 111

健康检查:

健康检查间隔(s):  秒 ?

健康阈值(次):  次 ?

不健康阈值(次):  次 ?

健康检查IP: 27.155.93.64/27  
59.153.74.128/25  
120.221.146.0/24  
140.249.26.0/24  
119.167.167.0/24

[返回目录](#)

## 源站配置

1. 在转发设置列表中，单击某项记录中的源站配置。

高防IP: [选择]

数据统计 | 七层配置 | **四层配置** | CC防护设置 | 证书管理 | 详细信息

CNAME: [选择].com

<input type="checkbox"/> 转发协议	服务端口	CNAME	真实服务器个数	健康检查
<input type="checkbox"/> TCP	80	[选择].com	1	开启

2. 在弹窗中，可对已有配置进行修改，单击添加源站配置，可新增一条配置信息。

### 源站配置

服务端口: 80

<input type="checkbox"/> 源站类型	服务器IP	服务器端口	健康检查状态	操作
非金山云	<input type="text" value="120.0.0.1"/>	<input type="text" value="80"/>	103.41.164.231(BGP)正常	<input type="button" value="确定"/> <input type="button" value="取消"/>

3. 单击确定，配置成功。

[返回目录](#)

## CC防护设置

本文档介绍了CC防护设置的基本操作步骤。

### 目录

#### 高防级别

- [开启\(关闭\)CC防护](#)

#### 域名记录级别

- [开启\(关闭\)CC防护](#)
- [添加自定义CC防护规则](#)
- [修改CC防护设置](#)

#### 高防级别

##### 开启(关闭)CC防护

1. 选择一个高防IP实例。
2. 展开更多列表，单击开启CC防护。

云安全 > 高防IP > 全部项目

高防名称	高防IP	链路类型	防护套餐	防护状态	转发配置	所属项目
<input checked="" type="checkbox"/> ksc_kad	(BGP)	静态BGP(华北)	30G/300G/503个端口	高防 已开启 CC 已关闭	七层 0个 四层 0个	test
<input type="checkbox"/> ksc_kad	(电信)	电信 (华北)	30G/300G/102个端口	高防 已开启 CC 已关闭	七层 0个 四层 0个	test
<input type="checkbox"/> ksc_kad	(BGP)	静态BGP(华北)	30G/300G/101个端口	高防 已开启 CC 已关闭	七层 2个 四层 0个	test

注意：请确定高防IP状态为“开启”

关闭CC防护同理，单击关闭CC防护

[返回目录](#)

### 域名记录级别

#### 开启(关闭)CC防护

1. 选择一个高防IP实例。
2. 在底部滑出面板中，单击进入CC防护设置页卡。
3. 选择要开启CC防护的域名记录，单击开启按钮。

注意：请确定高防IP的状态为“开启”，且CC防护状态为“开启”

云安全 > 高防IP > 全部项目

高防名称	高防IP	链路类型	防护套餐	防护状态	转发配置	所属项目
<input type="checkbox"/> ksc_kad	(BGP)	静态BGP(华北)	30G/300G/503个端口	高防 已开启 CC 已开启	七层 0个 四层 0个	test
<input type="checkbox"/> ksc_kad	(电信)	电信 (华北)	30G/300G/102个端口	高防 已开启 CC 已关闭	七层 0个 四层 0个	test
<input checked="" type="checkbox"/> ksc_kad	(BGP)	静态BGP(华北)	30G/300G/101个端口	高防 已开启 CC 已开启	七层 2个 四层 0个	test
<input type="checkbox"/> ksc_kad	(BGP)	静态BGP(华北)	30G/100G/100个端口	高防 已开启 CC 已关闭	七层 0个 四层 1个	默认项目

高防IP: (BGP)

域名记录级别

域名记录	请求阈值(QPS)	防护规则组	防护状态
<input checked="" type="checkbox"/> test.ksyun.com	120	无	开启
<input type="checkbox"/> www.zbuth.com	120	无	开启

关闭域名级别CC防护同理

[返回目录](#)

#### 添加自定义CC防护规则

1. 选择一个高防IP实例。
2. 在底部滑出面板中，单击进入CC防护设置页卡。

云安全 > 高防IP > 全部项目

高防名称	高防IP	链路类型	防护套餐	防护状态	转发配置	所属项目
<input type="checkbox"/> ksc_kad	██████████ (BGP)	静态BGP(华北)	30G/300G/503个端口	高防 已开启 CC 已开启	七层 0个 四层 0个	test
<input type="checkbox"/> ksc_kad	██████████ (电信)	电信 (华北)	30G/300G/102个端口	高防 已开启 CC 已关闭	七层 0个 四层 0个	test
<input checked="" type="checkbox"/> ksc_kad	██████████ (BGP)	静态BGP(华北)	30G/300G/101个端口	高防 已开启 CC 已开启	七层 2个 四层 0个	test
<input type="checkbox"/> ksc_kad	██████████ (3GP)	静态BGP(华北)	30G/100G/100个端口	高防 已开启 CC 已关闭	七层 0个 四层 1个	默认项目

高防IP: ██████████

域名记录级别

域名记录	请求阈值(QPS)	防护规则组	防护状态
<input checked="" type="checkbox"/> test.ksyun.com	120	无	开启
<input type="checkbox"/> www.zbuth.com	120	无	开启

- 单击**管理防护规则**按钮，进入CC防护规则页面。
- 单击**添加规则组**按钮，在弹出的对话框中填入规则组名称，单击**添加**。
- 选择第4步创建的规则组，在底部滑出面板中，单击**添加子规则**。
- 选择并填入规则信息，可添加针对ip、ua、referrer、path的自定义CC防护规则。

云安全 > 高防IP > BGP高防 > CC防护规则

规则组名称	状态
<input checked="" type="checkbox"/> test	开启

• 规则组名称: test

子规则

规则类型	规则数据	规则动作	规则状态	操作
ip	<input type="text"/>	放行	创建后默认不开启	确定 取消

ip  
ua  
referrer  
path

[返回目录](#)

### 修改CC防护设置

- 选择一个高防IP实例，单击**CC防护设置**页卡，进入CC防护设置。
- 选择要修改的域名记录，单击**编辑**。



云安全 > 高防IP > 全部项目

购买
开启
关闭
续费
升配
降配
新购防护包
删除
更多

高防名称	高防IP	链路类型	防护套餐	防护状态	转发配置	所属项目
<input type="checkbox"/> ksc_kad	[redacted] BGP)	静态BGP(华北)	30G/300G/503个端口	高防 已开启 CC 已开启	七层 0个 四层 0个	test
<input type="checkbox"/> ksc_kad	[redacted] 2(电信)	电信 (华北)	30G/300G/102个端口	高防 已开启 CC 已关闭	七层 0个 四层 0个	test
<input checked="" type="checkbox"/> ksc_kad	[redacted] (BGP)	静态BGP(华北)	30G/300G/101个端口	高防 已开启 CC 已开启	七层 2个 四层 0个	test
<input type="checkbox"/> ksc_kad	[redacted] (BGP)	静态BGP(华北)	30G/100G/100个端口	高防 已开启 CC 已关闭	七层 0个 四层 1个	默认项目

高防IP: [redacted]

数据统计
七层配置
四层配置
CC防护设置
证书管理
详细信息

域名记录级别 开启 关闭

域名记录	请求阈值(QPS)	防护规则组	防护状态
<input type="checkbox"/> test.ksyun.com	120	无	开启
<input type="checkbox"/> www.zbuth.com	120	无	开启

3. 进入编辑模式，可修改请求阈值和防护规则组

**请求阈值：**网站请求连接数（QPS）达到设置的阈值时，系统会对恶意攻击请求进行疑似判断并拦截，期间会对高度疑似攻击返回验证码以提高判断几率；如果实际请求连接数低于阈值则不会触发防御启动。

[返回目录](#)