目录

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

操作步骤

1. 登录高防IP控制台。
2. 选择要开启的高防IP实例，点击上侧的**开启**按钮。在弹出的确认框中点击**确定**。

3. 查看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

只有已过期的实例支持删除操作。

操作步骤

1. 登录高防IP控制台。
2. 选择要删除的高防IP实例，点击上侧的**删除**按钮。

3. 在弹出的确认框中单击**确定**。

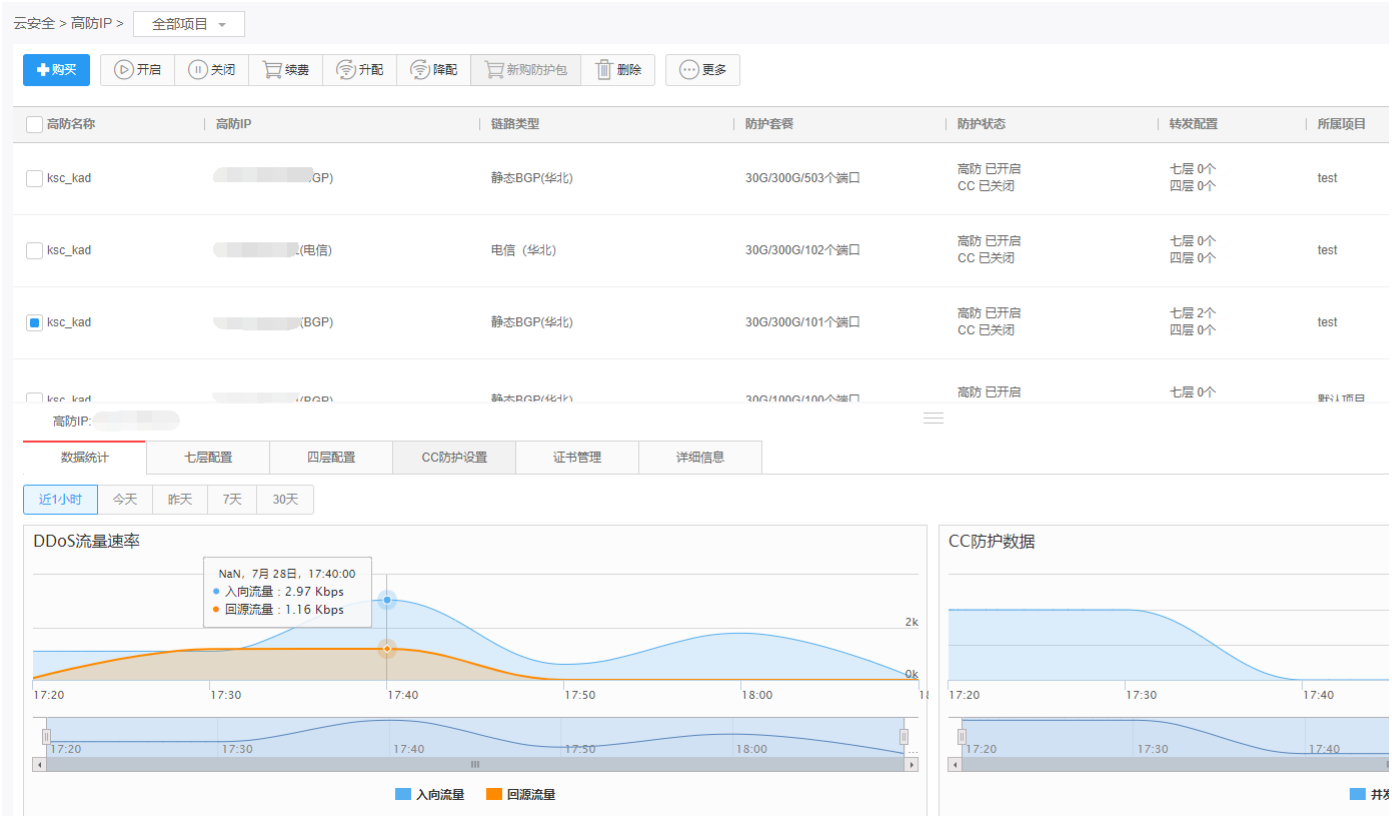
返回目录

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. 登录高防IP控制台。
2. 选择一个高防IP实例。
3. 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**：客户端对域名服务器发起的连接总数

七层配置

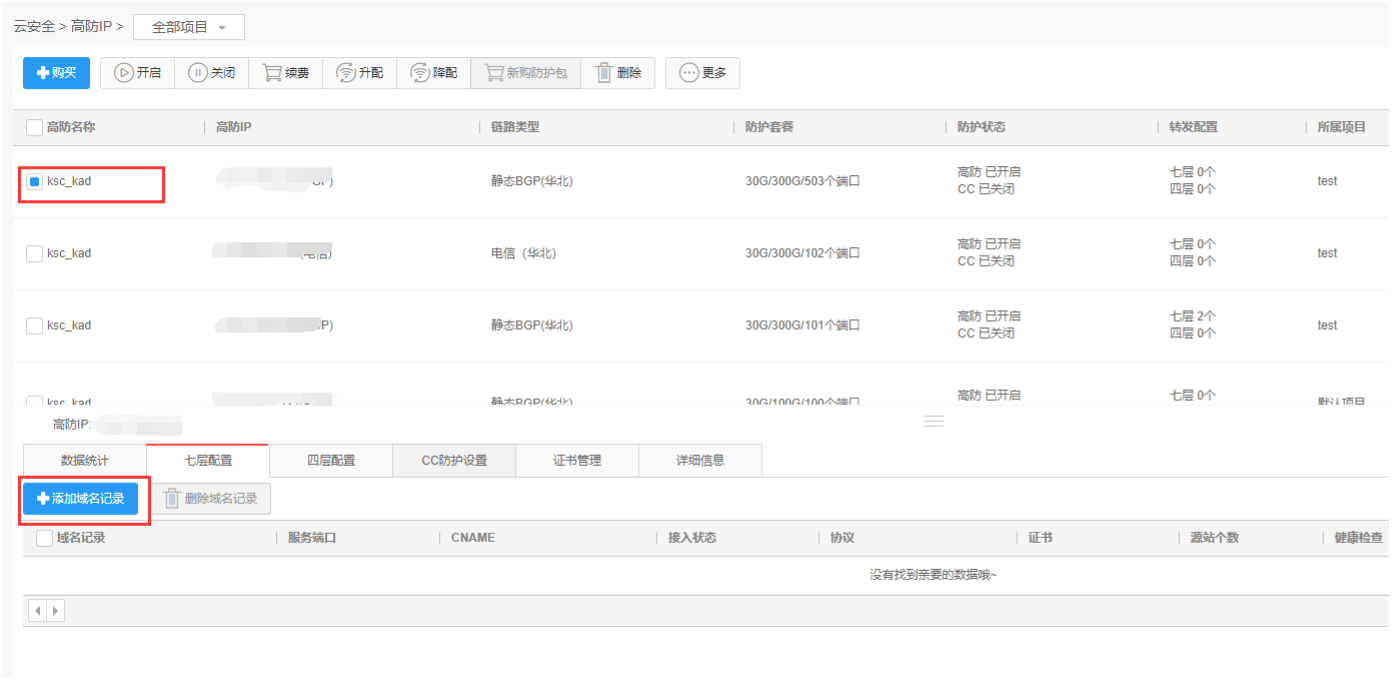
本文档介绍了网站业务接入的七层配置方式。

目录

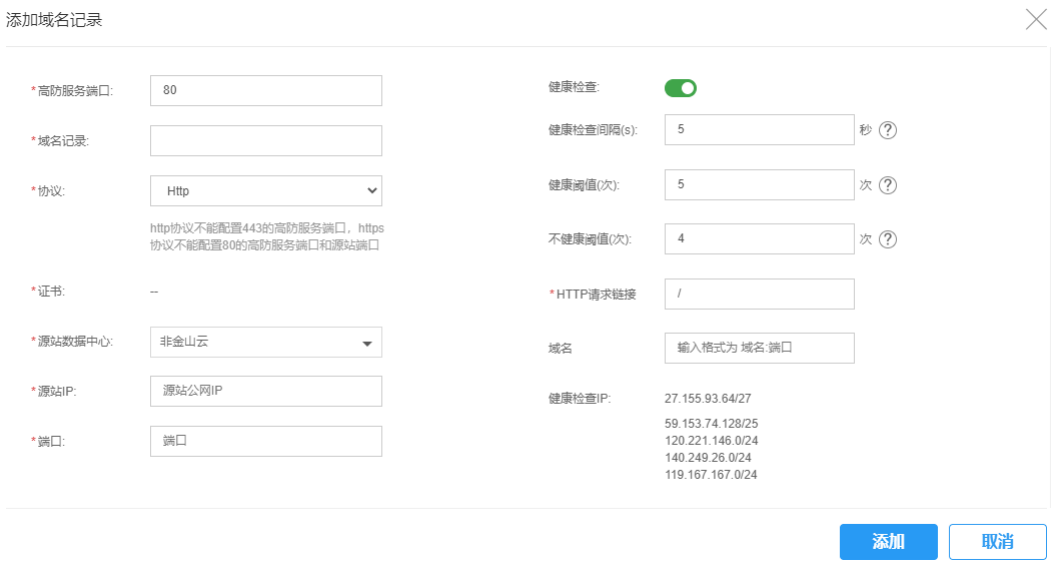
添加域名记录

操作步骤

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。



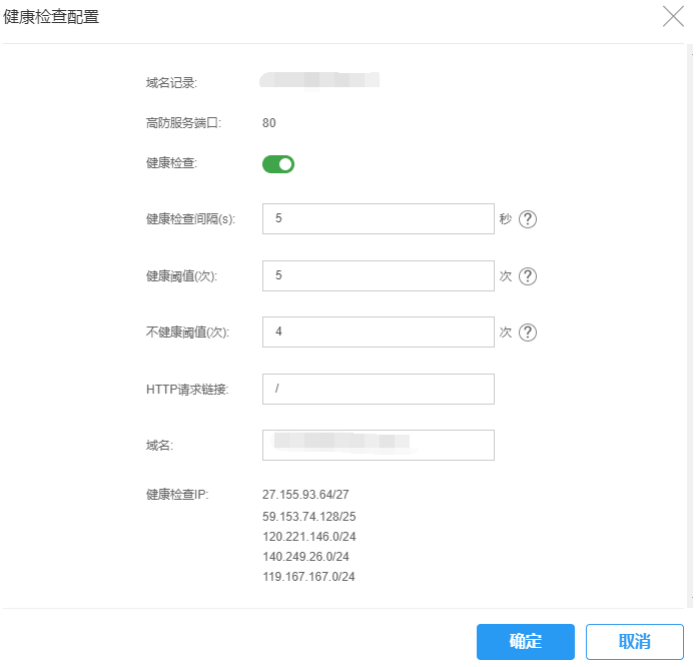
4. 点击**添加**，域名记录配置成功。

返回目录

健康检查配置

操作步骤

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。



3. 点击**确定**，完成健康检查配置。

返回目录

源站配置

操作步骤

1. 在域名记录中，点击**源站配置**。

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

配置导入与导出

高防IP支持导入或导出转发配置，有效降低您的业务迁移成本，提高使用效率。

操作步骤-导入

1. 选择高防IP实例，点击**七层配置**页签。
2. 点击**导入配置**按钮，在**导入七层配置**对话框中下载配置模板，并按照模板字段要求，填写相关信息。
3. 点击**选择文件**按钮，选择需要导入的文件。
4. 等待系统将导入数据解析至控制台后，点击**确定导入**按钮，完成导入操作。
5. 导入结果显示为**导入成功**，关闭对话框，导入配置成功。

操作步骤-导出

1. 选择高防IP实例，点击**七层配置**页签。
2. 点击**导出配置**按钮，即可将已配置的七层转发记录导出至excel文件。

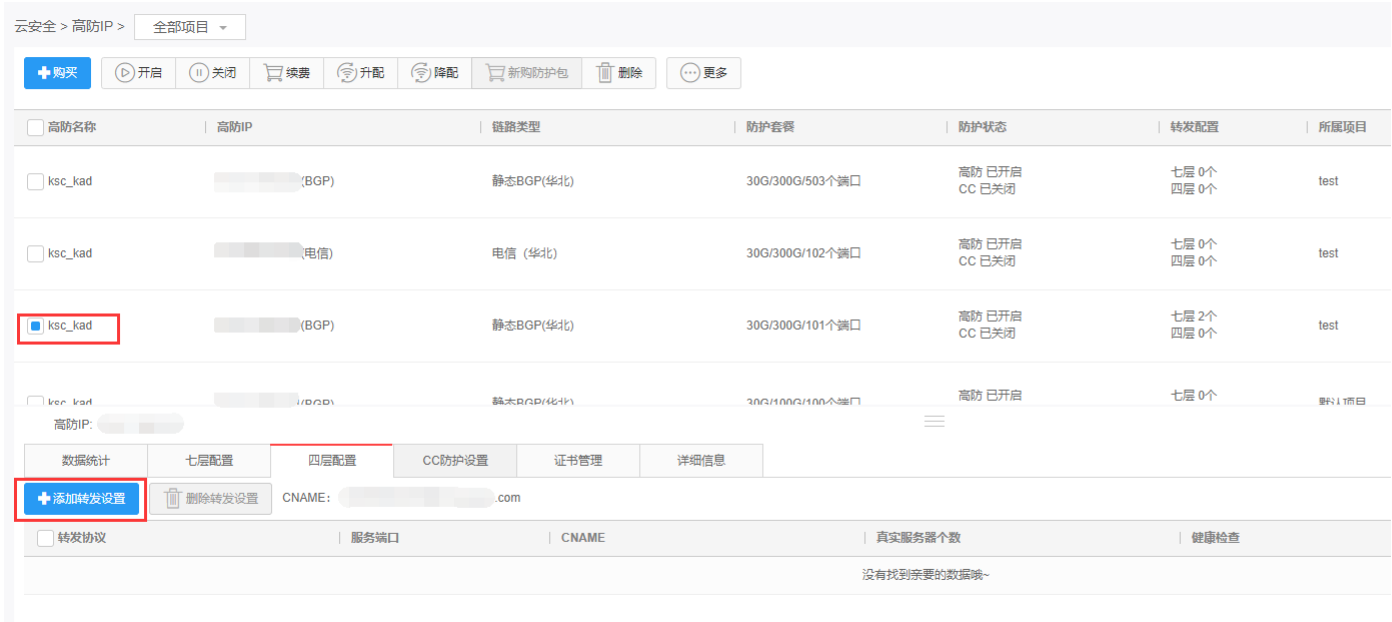
四层配置

本文档介绍了四层业务接入的配置方式。

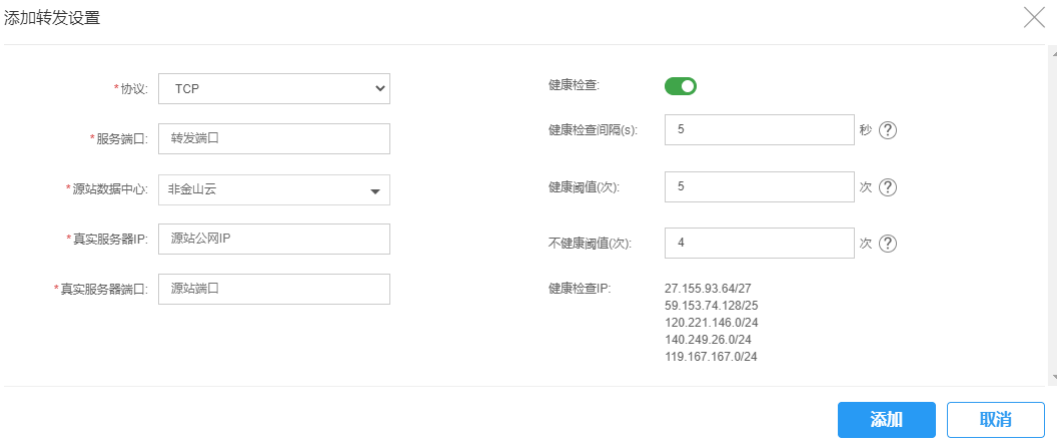
目录

添加转发设置

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。



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。

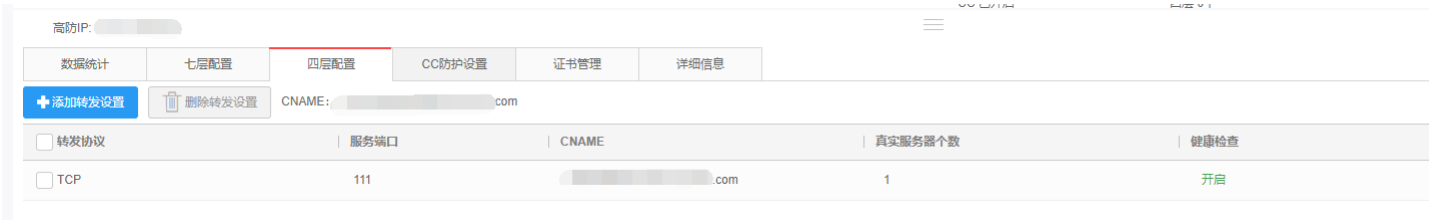


4. 单击**添加**，转发设置配置成功。

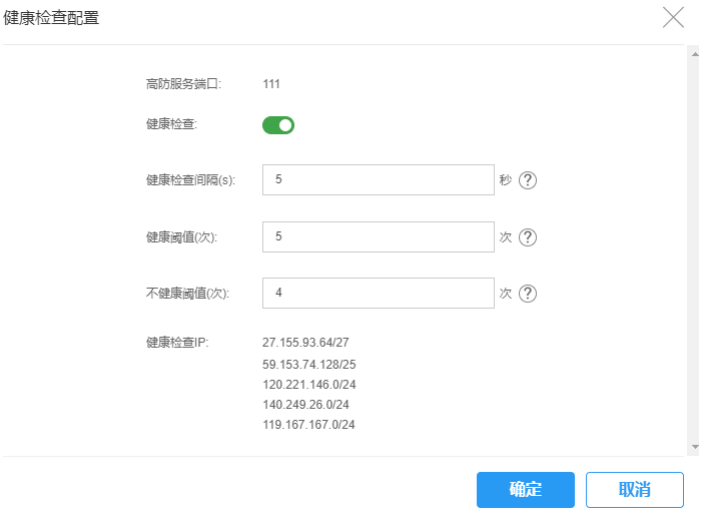
返回目录

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。



3. 点击确定，健康检查配置成功。



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**。

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。

3. 单击**确定**，配置成功。

返回目录

配置导入与导出

高防IP支持导入或导出转发配置，有效降低您的业务迁移成本，提高使用效率。

导入配置

1. 选择高防IP实例，点击**四层配置**页签。
2. 点击**导入配置**按钮，在**导入四层配置**对话框中下载配置模板，并按照模板字段要求，填写相关信息。
3. 点击**选择文件**按钮，选择需要导入的文件。
4. 等待系统将导入数据解析至控制台后，点击**确定导入**按钮，完成导入操作。
5. 导入结果显示为**导入成功**，关闭对话框，导入配置成功。

导出配置

1. 选择高防IP实例，点击**四层配置**页签。
2. 点击**导出配置**按钮，即可将已配置的四层转发记录导出至excel文件。

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

1. 选择一个高防IP实例。
2. 展开**更多**列表，单击**开启CC防护**。

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**

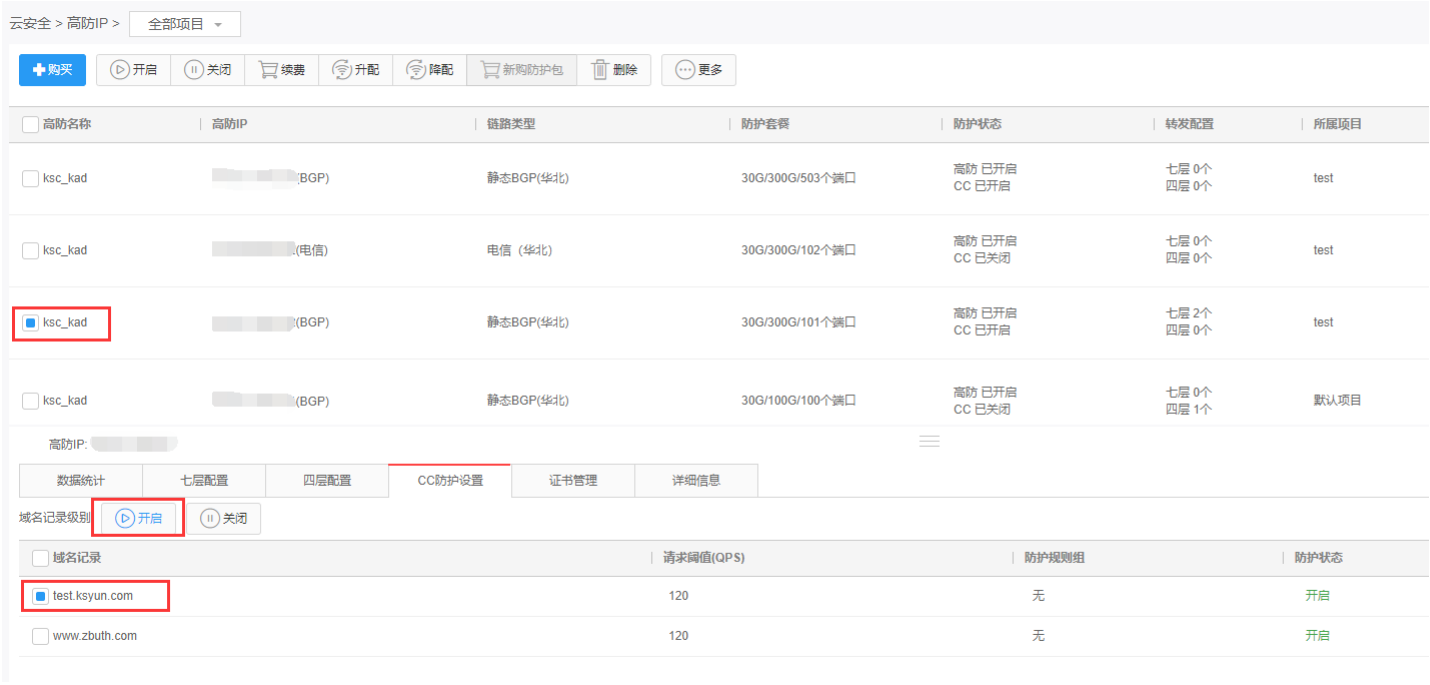
返回目录

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”

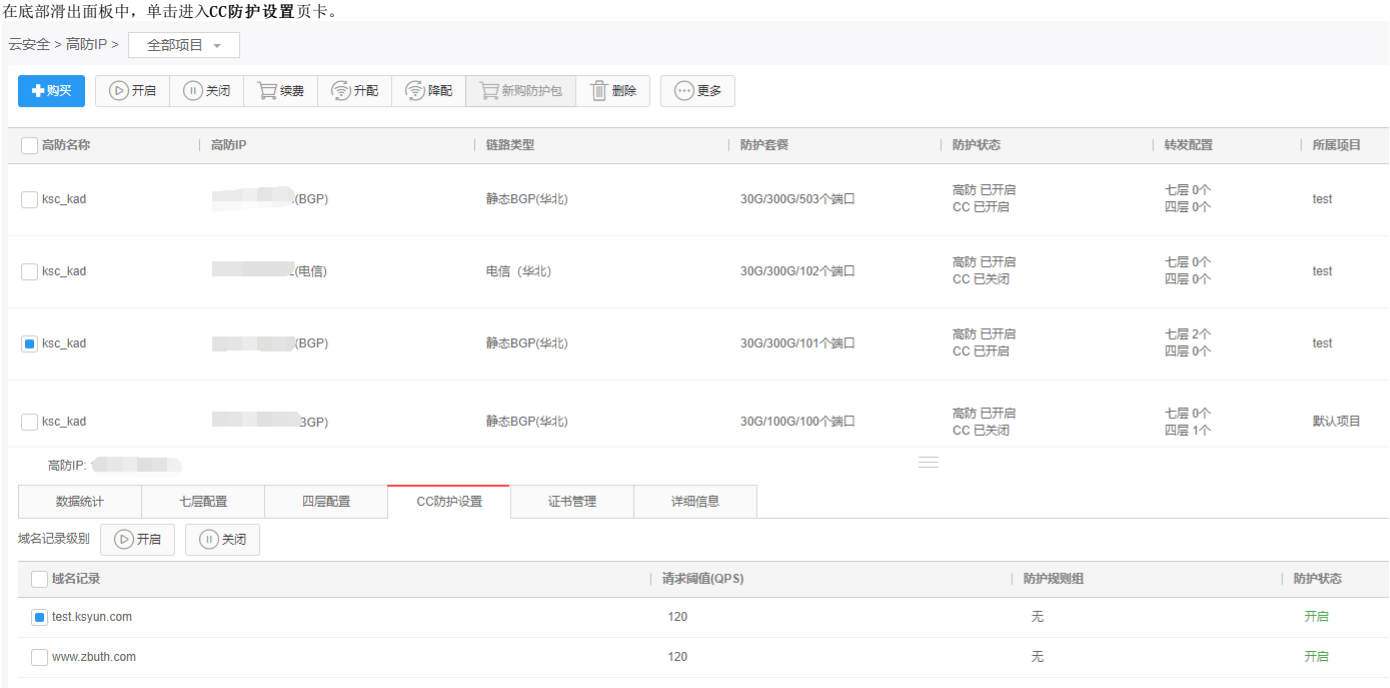


关闭域名级别CC防护同理

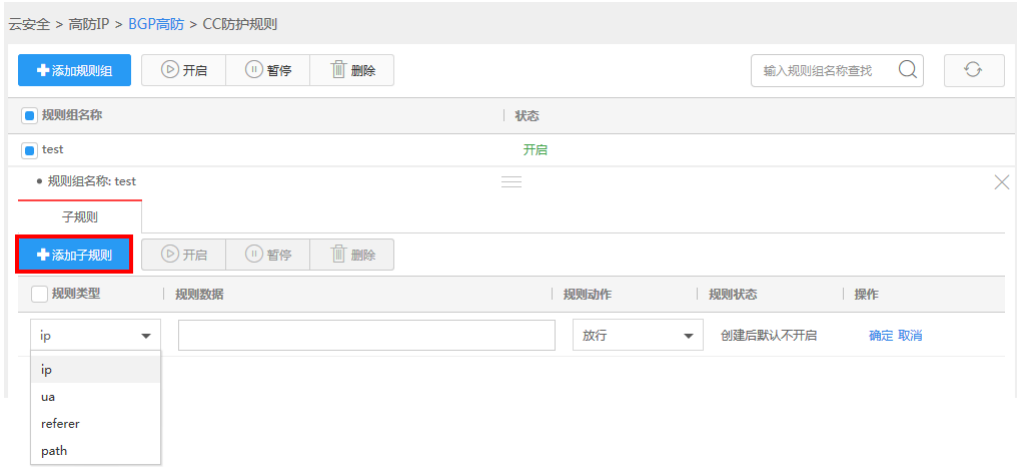
返回目录

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。



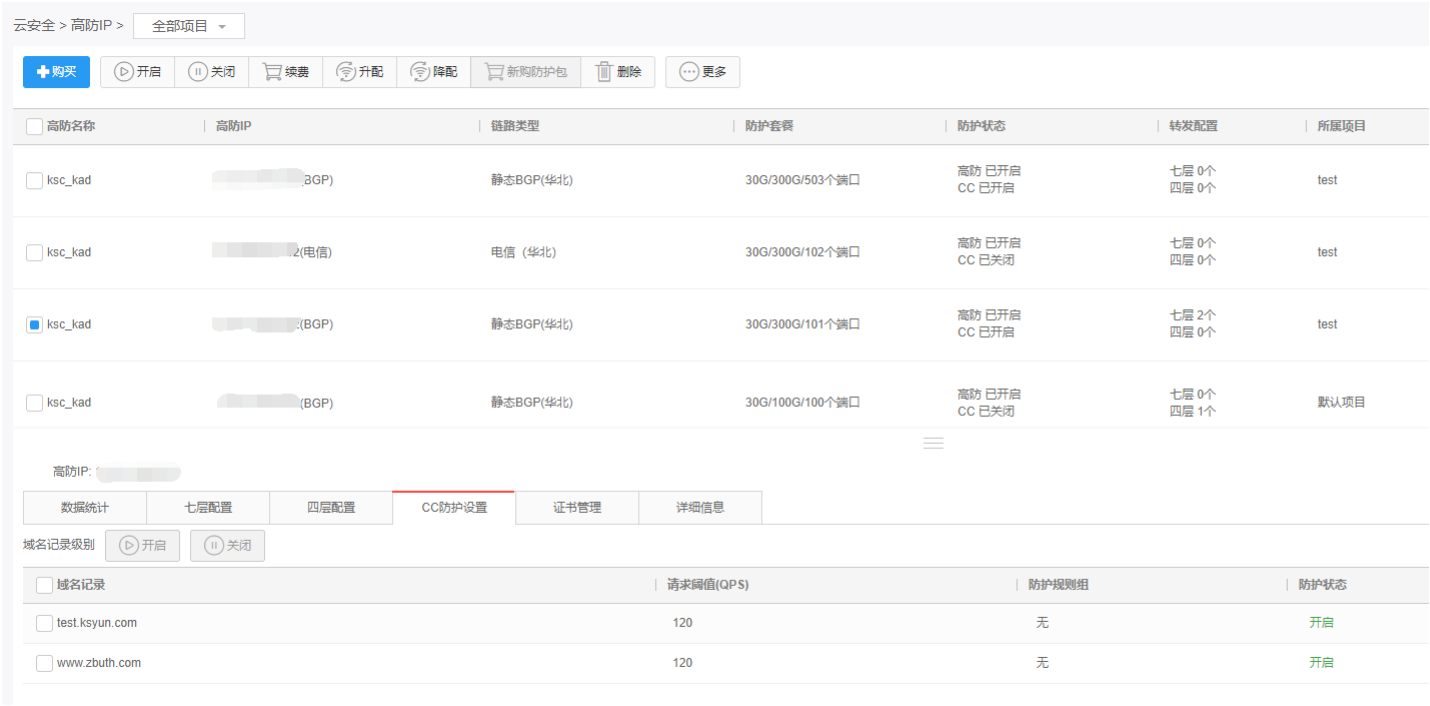
3. 单击**管理防护规则按钮**，进入CC防护规则页面。
4. 单击**添加规则组**按钮，在弹出的对话框中填入规则组名称，单击**添加**。
5. 选择第4步创建的规则组，在底部滑出面板中，单击**添加子规则**。
6. 选择并填入规则信息，可添加针对ip、ua、referrer、path的自定义CC防护规则。



返回目录

修改CC防护设置

1. 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。
2. 选择要修改的域名记录，单击**编辑**



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阀值则不会触发防御启动。

返回目录