DDoS 高防 IP

最佳实践

产品文档

腾讯云

版权所有：腾讯云计算（北京）有限责任公司

【版权声明】

©2013-2024 腾讯云版权所有

本文档著作权归腾讯云单独所有，未经腾讯云事先书面许可，任何主体不得以任何形式复制、修改、抄袭、传播全部或部分本文档内容。

【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。

【服务声明】

本文档意在向客户介绍腾讯云全部或部分产品、服务的当时的整体概况，部分产品、服务的内容可能有所调整。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。

文档目录

版权所有：腾讯云计算（北京）有限责任公司

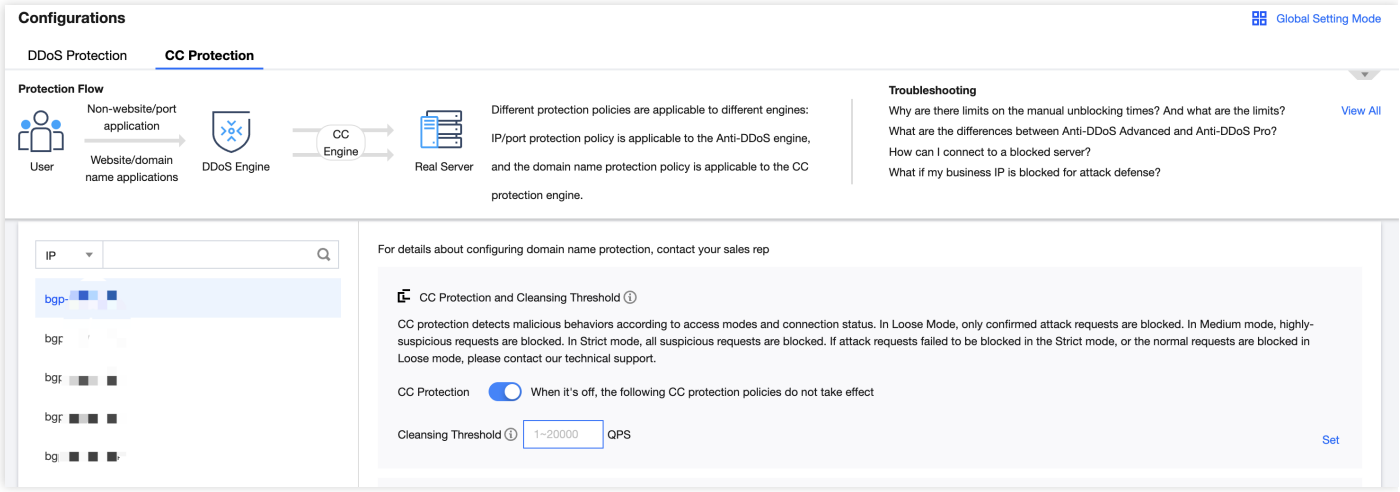
最佳实践
CC 防护策略配置流程及注意事项

最近更新时间：2022-08-16 15:28:12

DDoS 高防 IP 提供针对 CC 攻击的防护功能，策略包括防护等级、清洗阈值、精准防护、CC 频率限制等。业务完成接入后，您可以参考本文介绍的 CC 攻击防护策略配置流程，进行相关的配置，更好地保护您的业务。

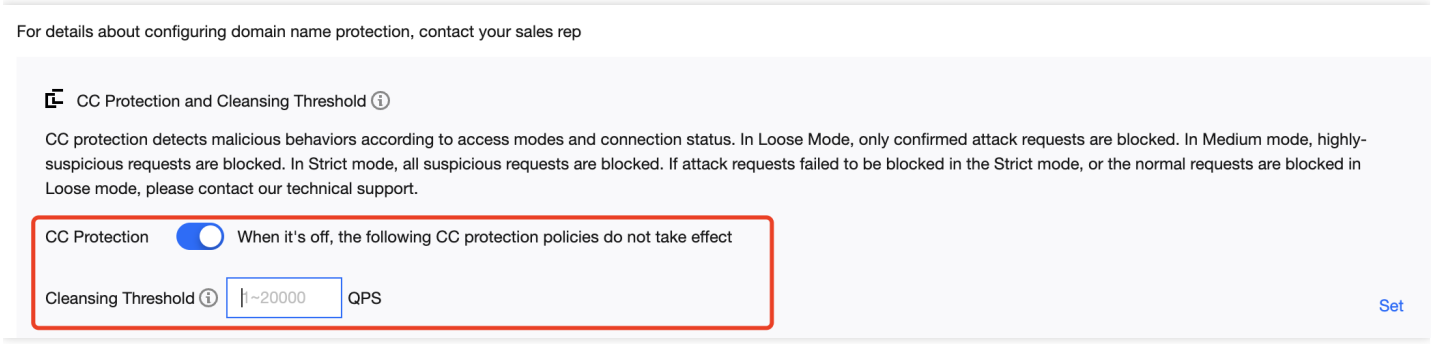
配置步骤

1. 登录 DDoS 高防 IP（新版）控制台，在左侧导航中，单击**防护配置** > **CC 防护**。
2. 在左边的列表选中高防 IP 的 ID 下面的域名，如"212.64.xx.xx bgpip-000002je" > "http:80" > "www.xxx.com"。



3. **CC 防护开关及清洗阈值**。在右侧选择 CC 防护开关及清洗阈值卡片，单击  开启开关，并设置 CC 防护清洗阈值。

> 说明：
>
> - 清洗阈值是 DDoS 高防的 CC 防护开关，具体的阈值可以设置为正常业务峰值的1.5倍。
> - 如果没有设置具体的阈值，高防 IP 将不会触发清洗动作，即 CC 防护为关闭状态。当存在 CC 攻击时，控制台所配置的防护等级、精准防护、CC 频率限制相关策略也不会生效，详细说明请参见 CC 防护开关及清洗阈值。

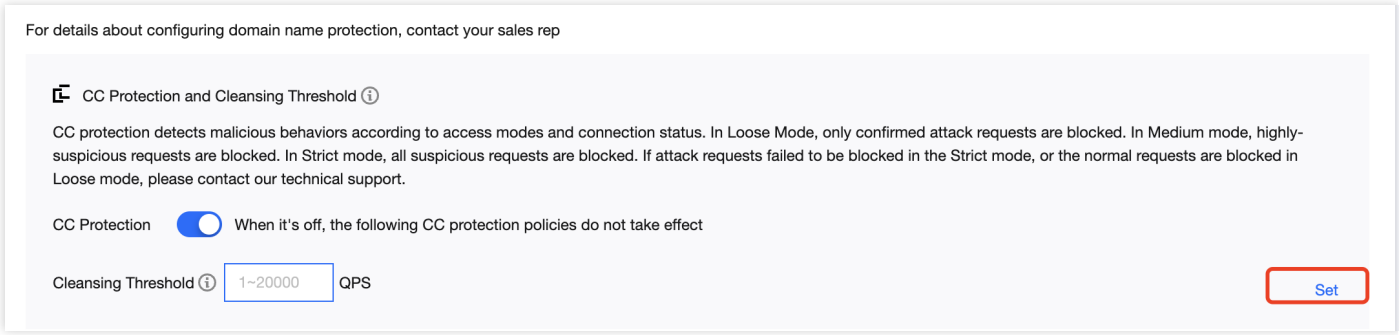


5. **精准防护策略配置**。

攻击发生时，建议通过网络抓包、中间件访问日志、其他防护设备等途径获取攻击请求的具体信息，并结合业务确定攻击特征，完成精准防护策略的配置。

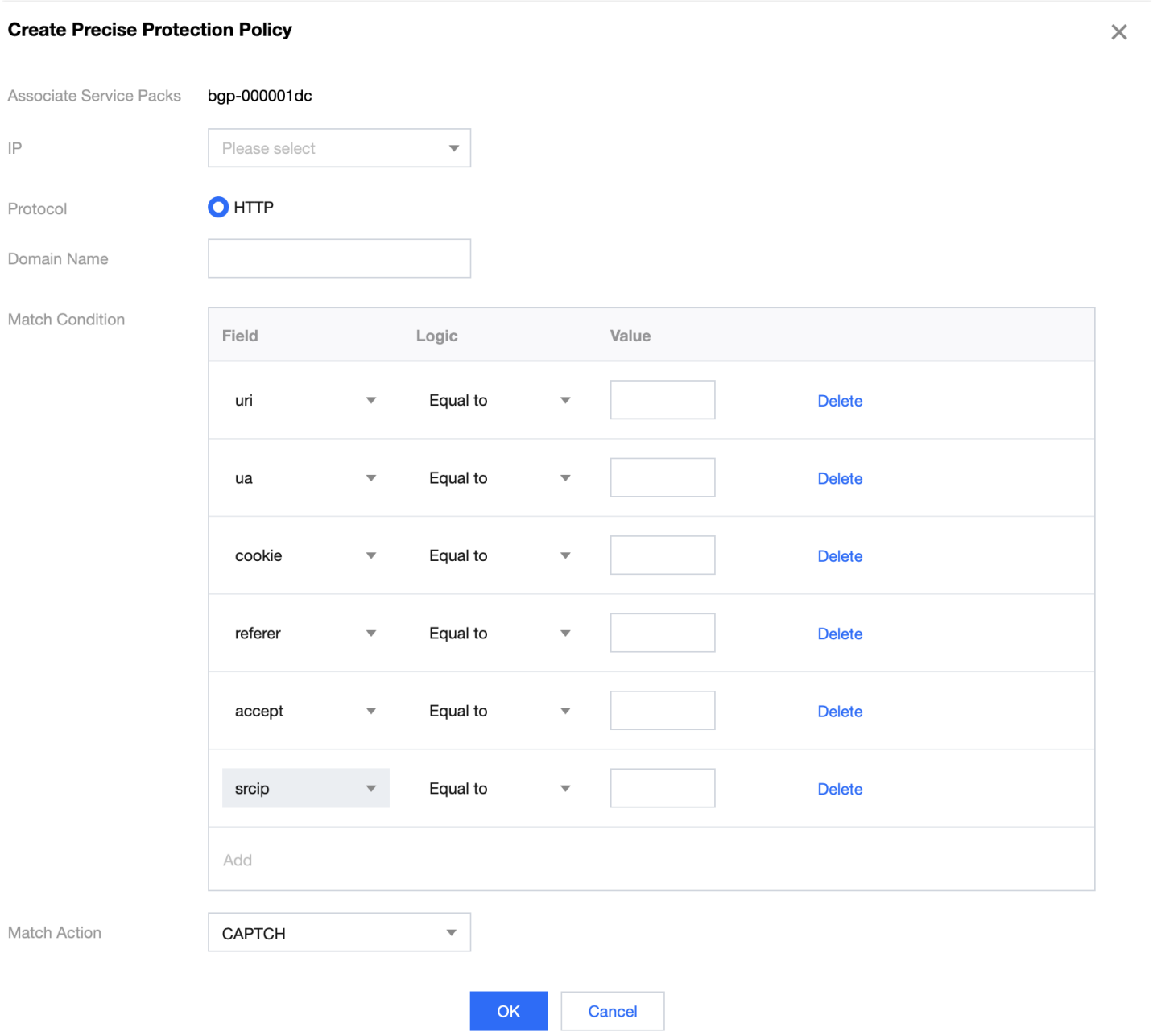
开启精确访问控制后，您可以对常见的 HTTP 字段（例如 URI、UA、Cookie、Referer 及 Accept 等）做条件组合防护策略，筛选访问请求，并对命中条件的请求设置人机校验或丢弃的策略动作。

1. 在 CC防护 页面的精准防护卡片中，单击**设置**，进入精准防护规则列表。



2. 单击**新建**，创建精准防护规则，填写相关字段，填写完成后，单击**确定**即可。详细配置说明，请参见 精准防护。

> 注意：
>
> - 如果同一条策略中，存在多个 HTTP 字段时，需所有条件都满足才能匹配到此条策略。
> - DDoS 高防 IP 可支持 HTTPS 业务的精准防护配置。



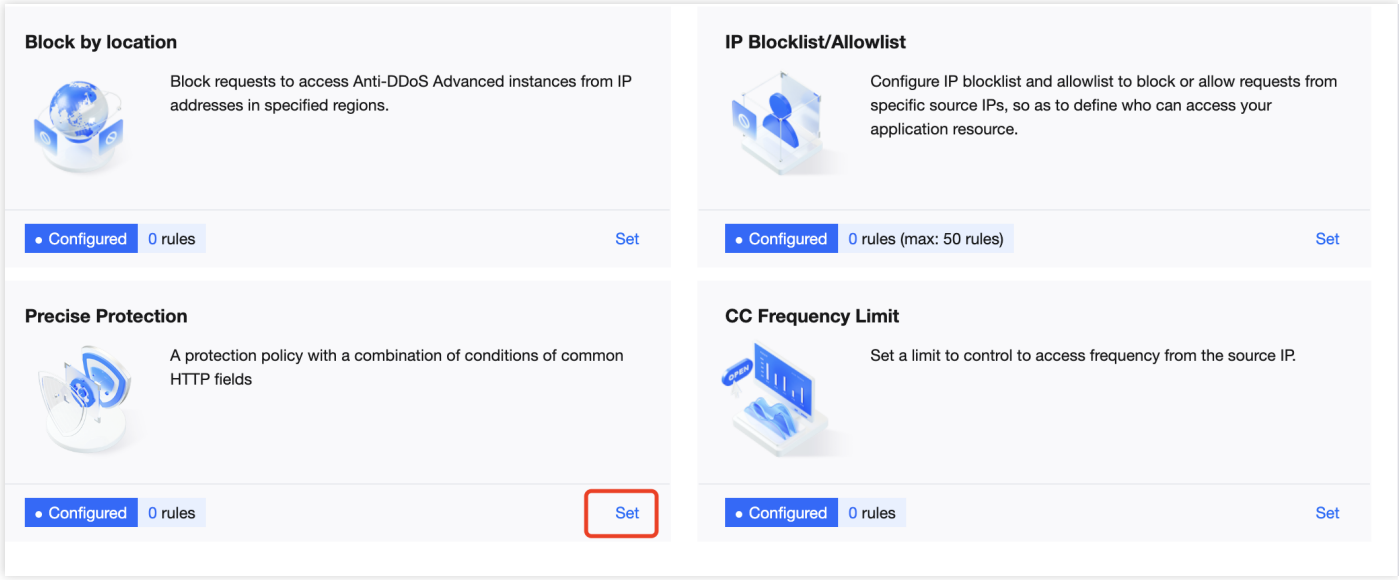
字段说明：

字段	字段描述
uri	访问请求的 URI 地址。
ua	发起访问请求的客户端浏览器标识等相关信息。
cookie	访问请求中的携带的 Cookie 信息。
referer	访问请求的来源网址，即该访问请求是从哪个页面跳转产生的。
accept	发起访问请求的客户端希望接受的数据类型。

版权所有：腾讯云计算（北京）有限责任公司

字段	字段描述
匹配条件	人机校验和丢弃， • 丢弃：不做人机识别，直接丢弃。 • 人机校验：采用通过算法进行人机识别。

6. **CC 频率限制**。
   DDoS 高防为已接入防护的网站业务提供频率控制防护策略，支持限制源 IP 的访问频率。您可以自定义频率控制规则，检测到单一源 IP 在短期内异常频繁地访问某个页面时，将设置人机校验或丢弃策略。
7. 在 CC防护 页面的 CC 频率限制卡片中，单击**设置**，进入精准防护规则列表。

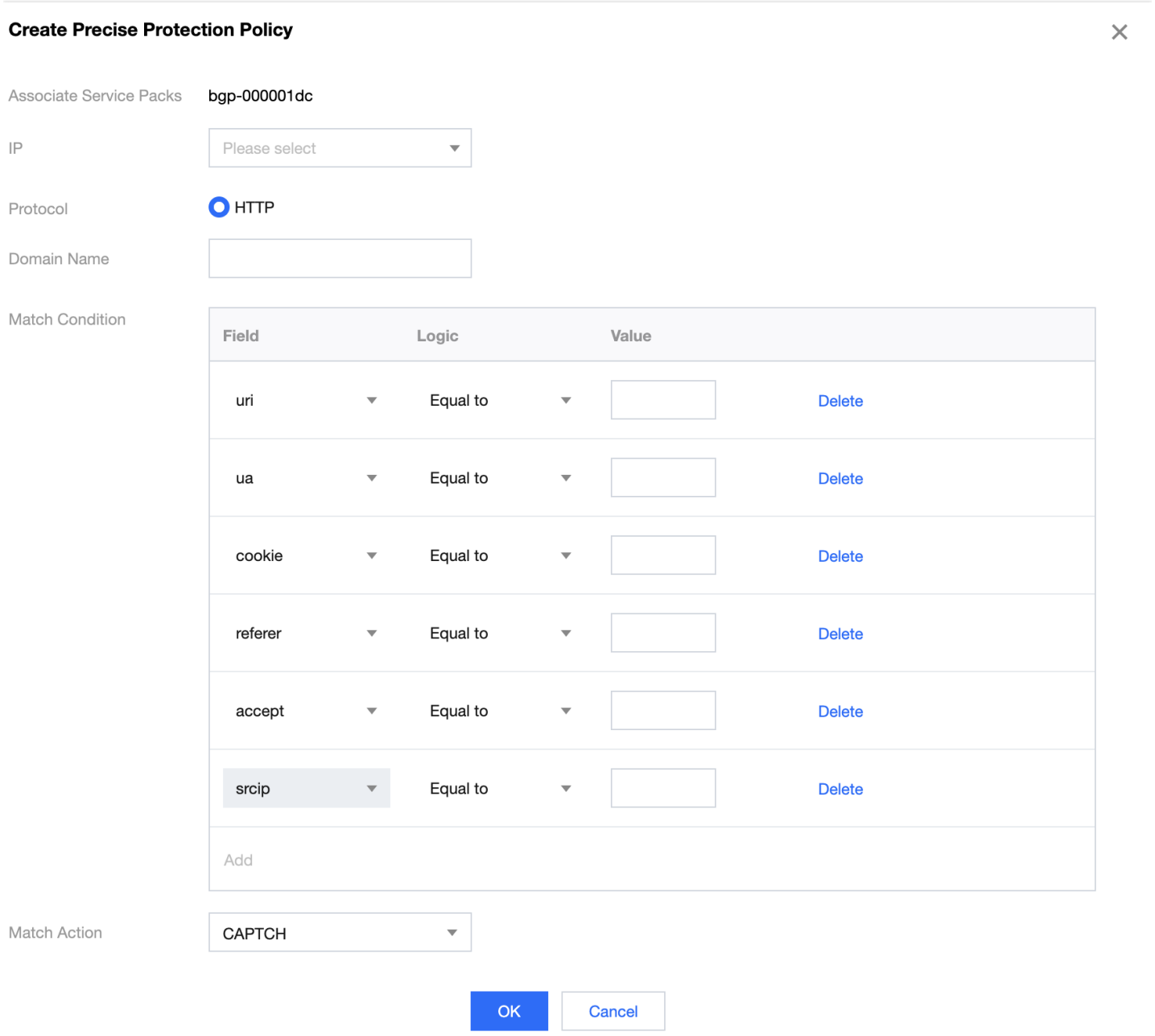


8. 单击**新增规则**，创建频率控制规则，填写相关字段，单击**确定**即可。详细配置说明，请参见 CC 频率控制。

注意：

- 在配置针对 URI 的 CC 频率限制策略时，需首先配置“/”目录的频率限制，且匹配模式必须设置为等于，配置“/”目录后,才能设置其他目录的 URI 访问频率限制。
- 配置“/”目录的频率限制的具体效果体现为在单位时间内，单个源 IP 请求此域名的“/”目录频率超过阈值，则触发相应的策略动作（人机校验或丢弃）。
- 每个域名在配置“/”目录的频率限制策略后，其他目录的检测时间必须保持一致。
- 当请求 URI 中存在不固定字符串时，可通过匹配模式包含配置来解决，即对 URI 中相同的前缀进行匹配。

版权所有：腾讯云计算（北京）有限责任公司



字段说明：

字段	字段描述
Cookie	访问请求中的携带的 Cookie 信息。
User-Agent	发起访问请求的客户端浏览器标识等相关信息。
Uri	访问请求的 URI 地址。

字段	字段描述
频率限制策略	人机校验和丢弃， • 丢弃：不做人机识别，直接丢弃。 • 人机校验：采用通过算法进行人机识别。
检查条件	根据业务情况设置访问频次。建议输入正常访问次数的2倍 - 3倍，例如，网站人平均访问20次/分钟，可配置为40次/分钟 - 60次/分钟，可依据被攻击严重程度调整。
惩罚时间	最长为一天。

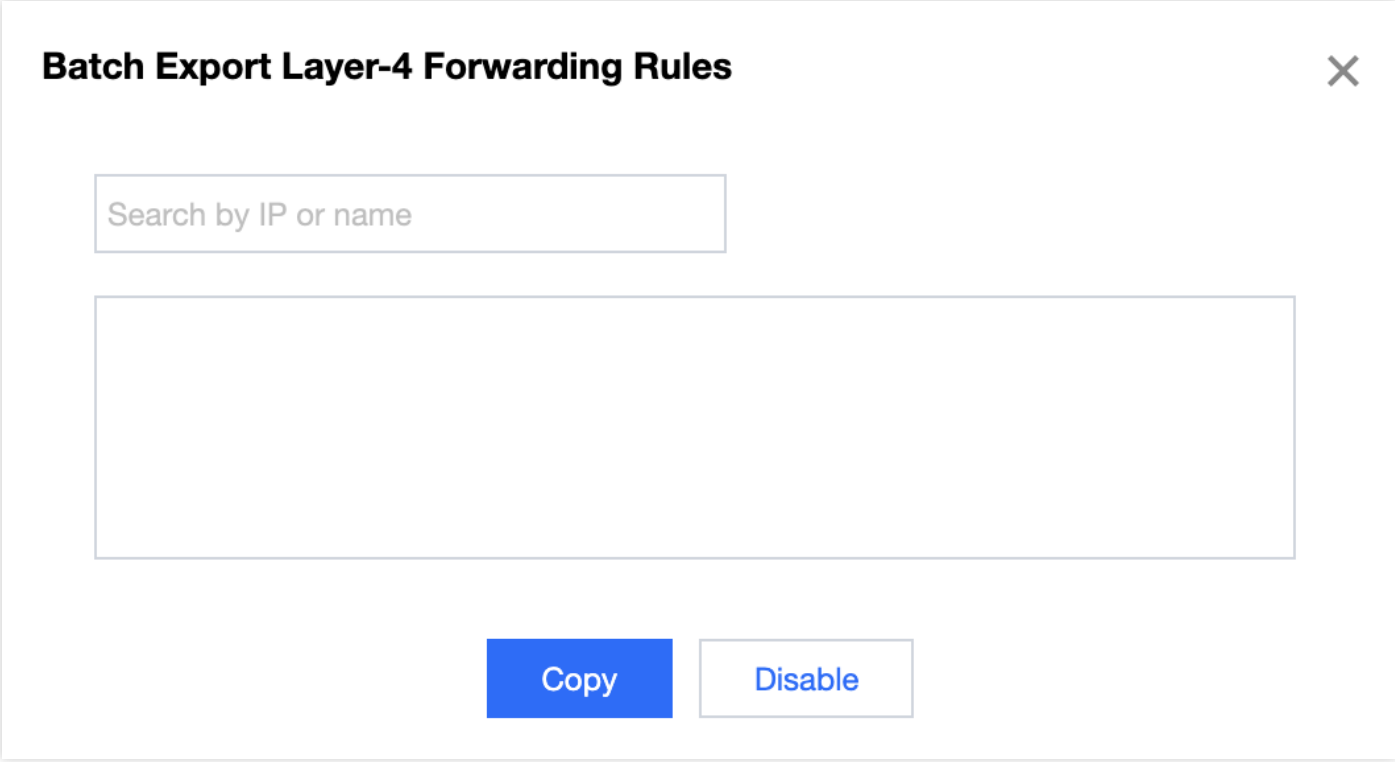
快速同步转发规则至新的高防 IP

最近更新时间：2022-06-10 14:12:06

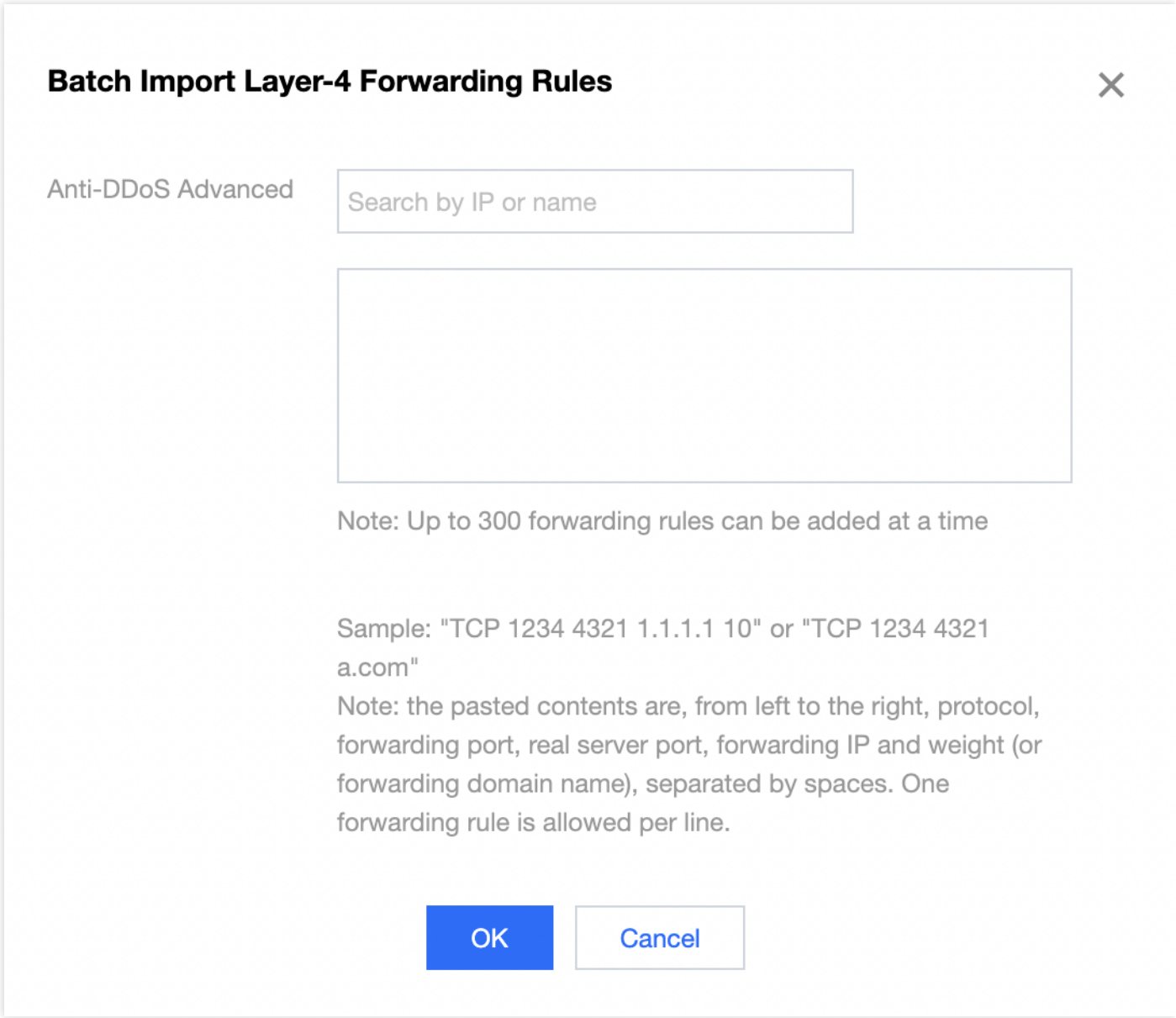
用户购买新的 DDoS 高防 IP 实例后，当实例数较多或配置三网高防 IP 实例时，如需以便捷的方式快速实现转发规则的同步，可参照本文档进行配置。

操作步骤

1. 登录 DDoS 高防 IP（新版）管理控制台，在左侧目录中，单击**业务接入 > 端口接入**。
2. 在端口接入页面，单击**批量导出**。
3. 在 IP 输入栏中，选择想要导出的高防 IP 转发规则后，会展示关于此高防 IP 已配置的转发规则，单击**复制**。



4. 在端口接入页面，单击**批量导入**。
5. 将新购买的高防 IP（未配置转发规则）输入到对应的输入栏，之后在下方的输入栏中，粘贴刚才已复制的内容，单击**确定**。



6. 在端口接入列表中，可以看到成功导入的转发规则。

通过智能调度实现三网流量调度

最近更新时间：2021-02-08 15:35:14

本文档将为您介绍如何通过智能调度实现三网流量调度。

操作场景

当 购买三网的高防 IP 后，比较常见的业务流量调度方式是根据 DNS 请求的运营商来源进行转发，即来自电信的流量调度到电信高防 IP、来自联通的流量调度到联通高防 IP、来自移动的流量调度到移动高防 IP、来自其他运营商的流量调度到优先级最高的高防线路，您可以通过配置智能调度，实现上述场景。

前提条件

- 在开启智能调度前，请将需要防护的业务接入高防实例进行防护。

> **说明：**
>
> - 若您需要将防护的云上产品 IP 添加至已购买的高防包实例，请参见 DDoS 高防包 快速入门。
> - 若您需要将四层或七层业务添加至已购买的 DDoS 高防 IP 实例，请参见 DDoS 高防 IP 端口接入 或 域名接入 。

- 在修改 DNS 解析前，您需要成功购买域名解析产品。

操作步骤

1. 登录 DDoS 高防 IP（新版）控制台，在左侧导航栏，单击【智能调度】，进入列表页面，单击【新建调度】，系统自动生成一个 CNAME 记录。
2. 找到该 CNAME 记录所在行，单击【添加高防实例】，进入智能调度编辑页面。
3. 在智能调度编辑页面中，TTL 值默认60秒，取值范围为1（秒）- 3600（秒），调度方式为默认优先级。
4. 单击【添加高防资源IP】，勾选需要设置智能调度的高防实例及IP，单击【确定】。
5. 选择高防实例后，实例的高防线路默认开启域名解析，再为其设置优先级。

> **说明：**
>
> - 三条运营商线路的优先级配置要相同，保证按照 DNS 请求的运营商来源进行响应。

版权所有：腾讯云计算（北京）有限责任公司

- 关于智能调度的配置，请参见 配置智能调度。

模拟 DDoS 攻击测试规则

最近更新时间：2022-08-29 10:58:27

购买了腾讯云高防包、高防IP或EdgeOne产品的客户如果想通过DDoS攻击来测试和确定您的应用或服务受到了应有的DDoS防护，您可以通过DDoS模拟测试来进行验证。

腾讯云允许使用腾讯高防包、高防IP、EdgeOne产品的客户进行DDoS模拟测试，但是DDoS模拟测试只能针对属于客户的应用和服务undefined 而且客户了解DDoS模拟测试的风险并对模拟测试人员的行为负责。为了降低模拟测试对生产网络环境的影响，我们建议DDoS模拟测试最好在您的测试网络环境或者选择在非高峰时段进行。

为了避免DDoS模拟测试对其他腾讯云用户造成影响，您必须提前至少3个工作日通知腾讯云团队并提供以下与测试相关的信息，并且您同意一旦收到腾讯云团队关于停止测试的要求便立即停止DDoS模拟测试。

- 发起攻击的地域
- 攻击时长
- 发起攻击时段
- 攻击手段/方法（可选）
- 攻击流量大小/范围
- 攻击的IP/范围/区域
- 攻击端口
- 攻击协议
- 最大数据包传输率
- 紧急联系人信息（姓名undefined 邮箱和手机号码）

版权所有：腾讯云计算（北京）有限责任公司