

DDoS 高防包

最佳实践

产品文档



腾讯云

【版权声明】

©2013-2023 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模式的承诺或保证。

文档目录

最佳实践

BGP 高防包异地防护方案

BGP 高防包与 Web 应用防火墙结合使用

业务系统压力测试建议

源站 IP 暴露的解决方法

CC 防护策略配置流程及注意事项

模拟 DDoS 攻击测试规则

高防 EIP 创建使用指引

最佳实践

BGP 高防包异地防护方案

最近更新时间：2020-07-07 16:10:32

需求背景

受客观因素影响，DDoS 高防包在北京、上海和广州可售卖的最大防护能力有所差异，上海可售卖的最大防护能力为 300Gpbs，广州和北京两地可售卖防护能力均小于上海。除此之外，中国内地（大陆）成都、重庆等区域尚未上线高防包产品。

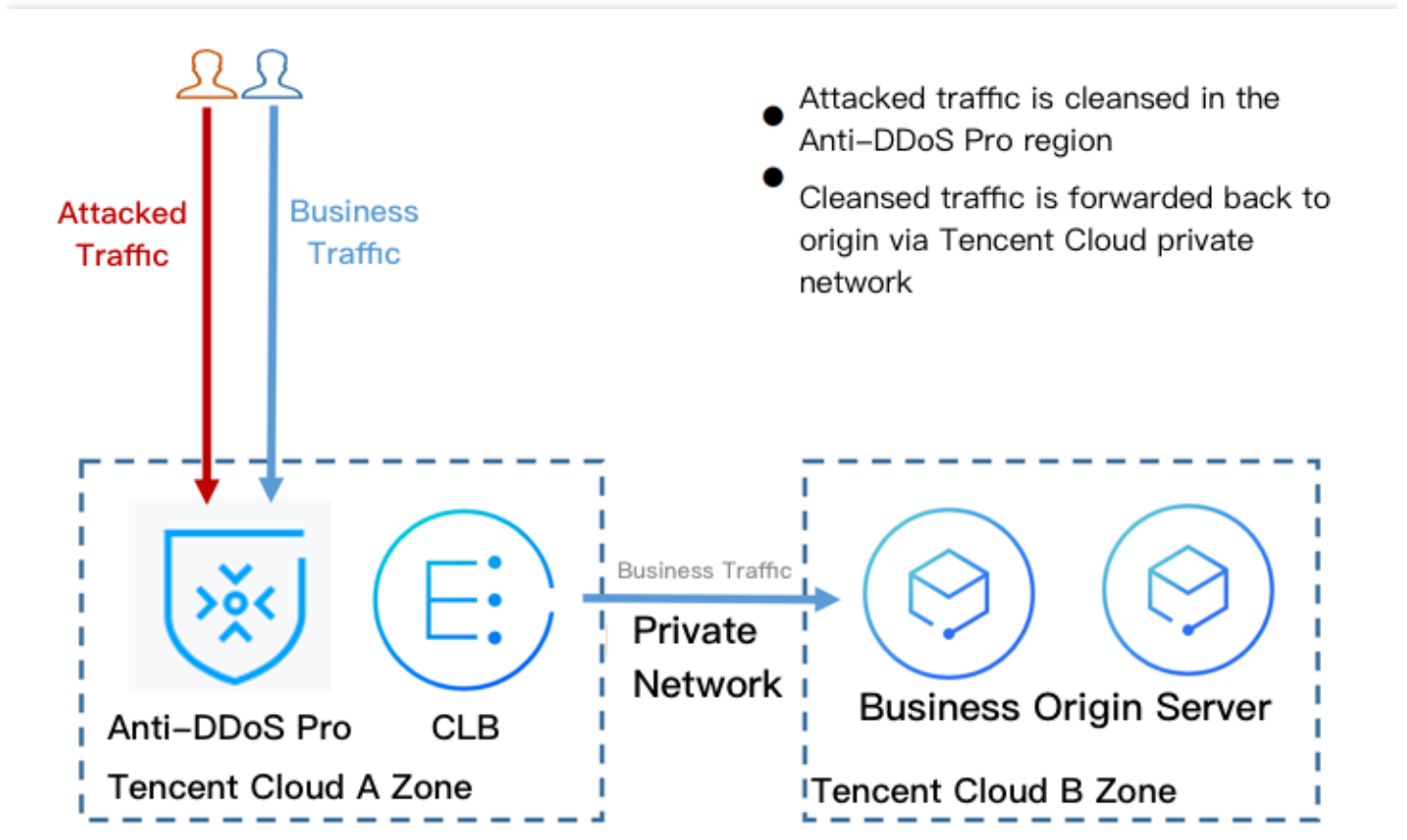
如果用户业务源站部署在腾讯云，并且需要使用腾讯云非源站所在地区的 DDoS 防护能力时，可参考本方案。

防护方案

本方案主要由 DDoS 高防包、CLB 负载均衡、源站业务 Server 组成。在具有 DDoS 高防包资源的地区部署 CLB 负载均衡，并将其与 DDoS 高防包进行绑定。配置 CLB 的内网回源规则，确保通过 CLB 的公网 IP 可以访问业务。

- 常态化情况下，业务可根据需要解析到源站业务的公网 IP（或直接解析到异地的 CLB 公网 IP），业务流量就近访问源站。
- 在发生攻击后，将业务解析到 CLB 的 IP，对 DDoS 攻击流量进行清洗，完成清洗后，由 CLB 通过内网专线将流量转发回到源站。

具体的防护方案如下图：



方案效果

- 打破地域防护能力的限制，可具有最大300Gpbs的 DDoS 高防包 DDoS 防护能力。
- 业务流量使用腾讯云的內网专线进行转发，可靠性高、延迟小。
- 充分享用腾讯云 DDoS 网络的优势，所有公网 IP 均为 BGP IP，延迟低。

建议与注意事项

- 提前部署 DDoS 高防包和 CLB 负载均衡。
- 建立业务可用性监测机制，在未部署自动切换机制的情况下，发现源站访问异常及时介入处理。
- 定期进行验证和演练，了解和熟悉方案细节，解决可能存在的问题。

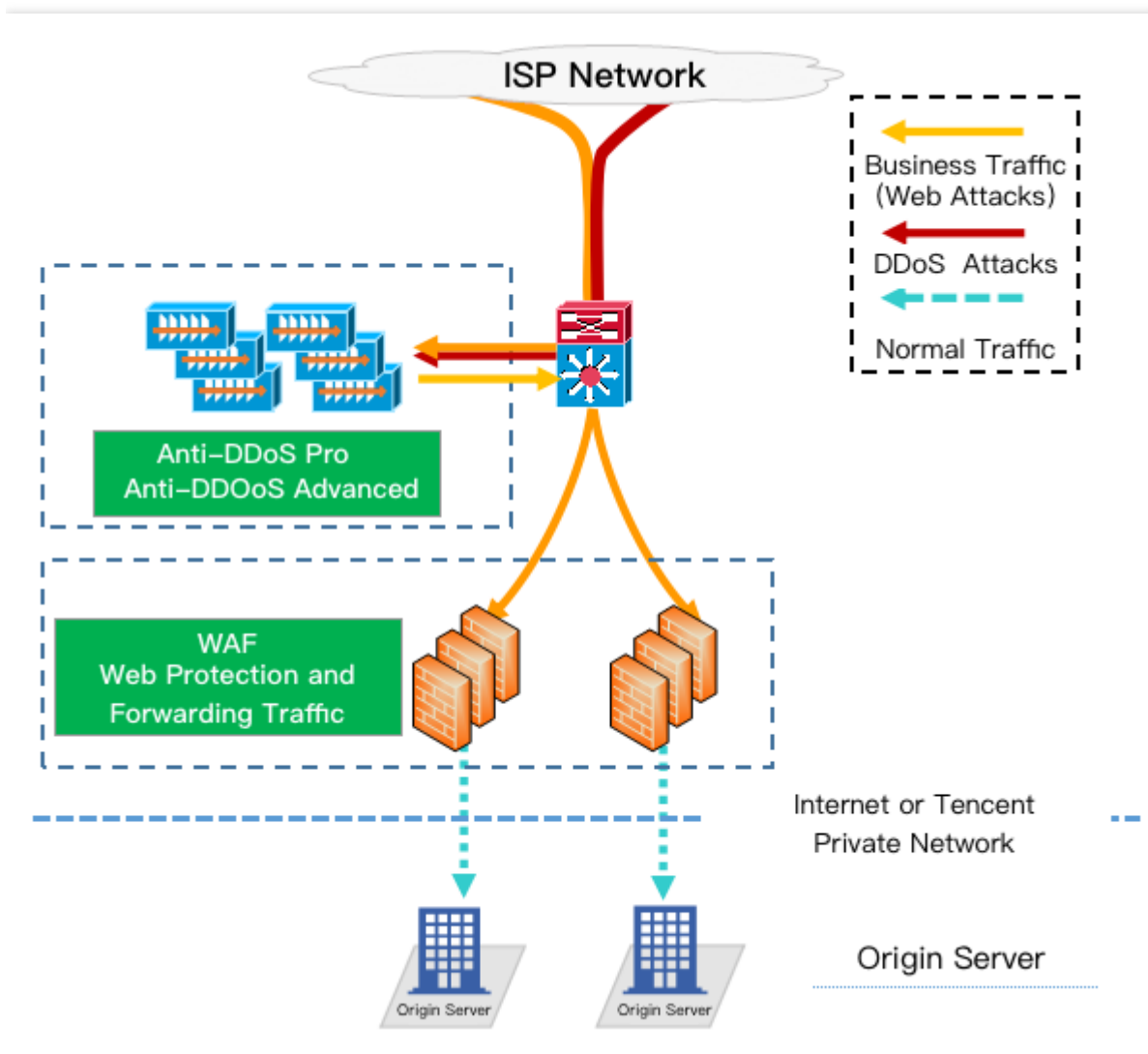
BGP 高防包与 Web 应用防火墙结合使用

最近更新时间：2021-08-17 11:10:38

DDoS 高防包支持联动 Web 应用防火墙，为用户提供全方位安全防护。

- DDoS 高防包一键提供上百 Gbps DDoS 防护能力，轻松应对 DDoS 攻击，保障业务稳定运行。
- Web 应用防火墙实时防护，有效拦截 Web 攻击行为，保障用户业务的数据和信息安全。

部署方案



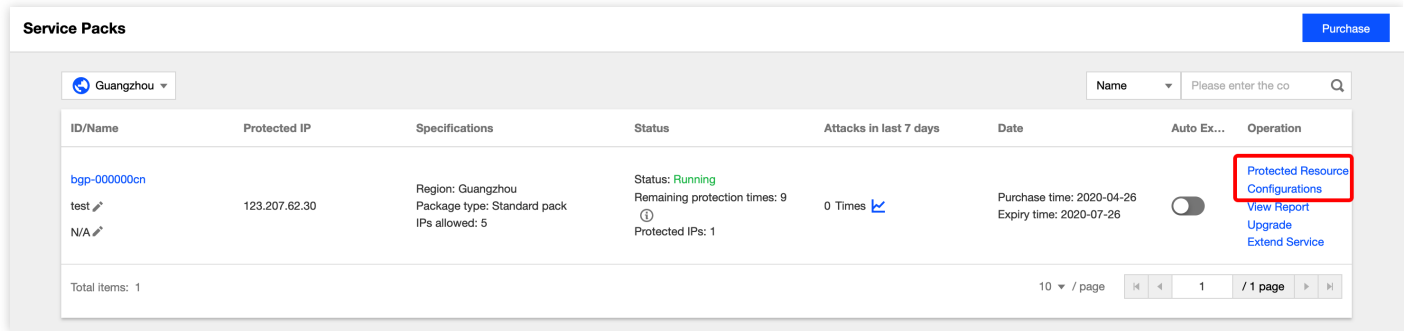
配置过程

配置 Web 应用防火墙

如需快速接入 Web 应用防火墙，详情请参见 [Web 应用防火墙快速入门](#)。

配置 DDoS 高防包

1. 登录 [DDoS 高防包（新版）控制台](#)，在左侧操作栏中，单击【高防包】。
2. 选择目的高防包实例所在地域，单击目的高防包实例所在行的操作项【管理防护对象】。



3. 在管理防护对象页面，根据实际防护需求选择“关联设备类型”与“选择资源实例”。
 - 关联设备类型：支持云服务器，负载均衡，Web 应用防火墙等公有云具有公网IP的资源。

- 选择资源实例：允许多选，选择资源实例数量不得超过“可绑定 IP 数”。

Protected Resource
✕

i Note: Configured protection policy only works to the currently bound IP. If the protection policy is not applicable to the current IP, please change it.

IP/Resource
Name test

Region Guangzhou

Max Bound
IPs 5

Resource Type Cloud Virtual Machine

Select resource

	Resource ID/Name	IP Address	Resource Type
<input checked="" type="checkbox"/>	ins-n9f01kte hrt-ceshi	123.207.62.30	Cloud Virtual Mach...
<input type="checkbox"/>	ins-rgcrtofc ulricwang-test2	129.204.214.5	Cloud Virtual Mach...
<input type="checkbox"/>	ins-r397nyvi ulricwang-test1	134.175.10.59	Cloud Virtual Mach...

Total items: 9

100 / page 1 / 1 page

Press Shift key to select more

Selected (1)

Resource ID/Na...	IP Address	Resource Type
ins-n9f01kte	123.207.62.30	Cloud Virtual Mac... ✕

OK
Cancel

4. 设置完成后，单击【确定】即可。

业务系统压力测试建议

最近更新时间：2022-07-06 14:31:54

压力测试过程在一定程度上与 DDoS 攻击类似，为确保压力测试取得相应效果，建议用户在进行压力测试前先参考本文档获取适用的建议，再拟定合适实施方案。

注意：

以下建议主要是基于 DDoS 防护对压力测试的影响而提出。其他与压力测试有关的方面，如网络带宽、链路负载或其他基础资源情况等，请用户结合实际情况考虑和补充。

调整防护策略

- 建议关闭 CC 防护策略，如存在某些客观原因不能关闭 CC 防护策略，请将 CC 攻击防护的 HTTP 请求数阈值调整到压测最大值以上。
- 建议关闭 DDoS 防护策略，如存在某些客观原因不能关闭 DDoS 防护策略，请将 DDoS 防护的清洗阈值调整到压测最大值以上。

控制压测流量及请求数

- 建议将压测流量值设置为小于1Gbps，否则将有可能触发攻击防护。
- 建议将压测的 HTTP 请求数限制在20,000QPS以内（即 HTTP 请求数每秒不超过20,000个），否则将有可能触发攻击防护。
- 建议将压测的每秒新建连接数小于50,000个，最大连接数小于2,000,000个，每秒入包量小于200,000个。

注意：

如压测需要超出以上限制范围，请联系 [腾讯云技术支持](#)，售后团队将配合进行压测工作。

提前评估压测可能的影响

建议用户在压测前联系腾讯云架构师或 [腾讯云技术支持](#)，全面评估压测可能产生的影响及范围，制定合理的风险规避措施。

源站 IP 暴露的解决方法

最近更新时间：2020-07-07 16:10:34

由于部分攻击者会记录源站使用过的 IP，因此在使用 BGP 高防包后存在绕过高防直接攻击源站 IP 的情况。如遇到以上情况，建议用户更换源站 IP。

在更换源站 IP 前可参考本文档，对暴露源站 IP 的可能因素进行检查，避免新更换的源站 IP 继续暴露。

检查方法

DNS 解析记录检查

检查该遭到攻击的旧源站 IP 上所有 DNS 解析记录，如子域名的解析记录、邮件服务器 MX（Mail Exchanger）记录以及 NS（Name Server）记录等，确保全部配置到高防 IP，避免部分解析记录直接解析成新更换的源站 IP。

信息泄露及命令执行类漏洞检查

- 检查网站或业务系统是否存在信息泄露的漏洞，如 phpinfo() 泄露、GitHub 信息泄露等。
- 检查网站或业务系统是否存在命令执行类漏洞。

木马或后门检查

检查源站服务器是否存在木马或后门等隐患。

其他建议

- 建议不使用与旧源站 IP 相同或相近网段的 IP 作为新的源站 IP，避免攻击者对 C 段或相近网段进行猜测和扫描。
- 建议提前准备备份链路和备份 IP。
- 建议设置访问来源范围，避免攻击者的恶意扫描。

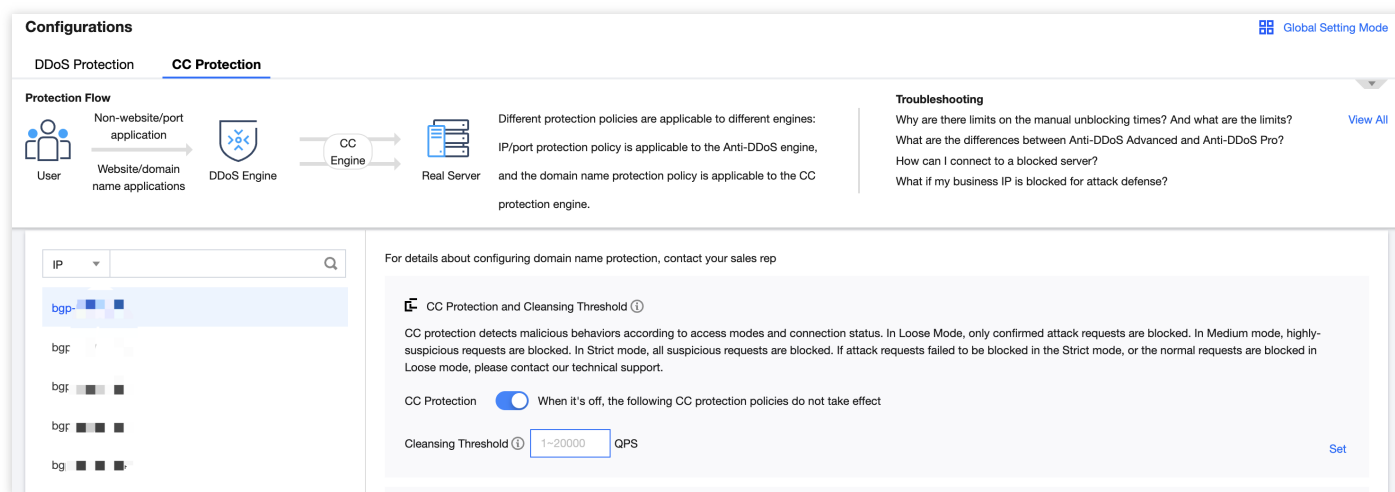
CC 防护策略配置流程及注意事项


最近更新时间：2022-06-13 17:14:23

DDoS 高防包提供针对 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。

步骤1：设置清洗阈值

1. 登录 [DDoS 高防包管理控制台](#)，在左侧导航中，单击**防护配置** > **CC防护**。
2. 在 CC 防护页面的左侧列表中，选中高防包的 ID，如“bgp-00xxxxxx”。



3. 在 CC 防护开关及清洗阈值卡片中，单击  开启 CC 防护开关，当防护开启后必须进行清洗阈值设置否则无法使用 CC 防护。

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，高防包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](#)。

For details about configuring domain name protection, contact your sales rep

CC Protection and Cleansing Threshold ⓘ

CC protection detects malicious behaviors according to access modes and connection status. In Loose Mode, only confirmed attack requests are blocked. In Medium mode, highly-suspicious requests are blocked. In Strict mode, all suspicious requests are blocked. If attack requests failed to be blocked in the Strict mode, or the normal requests are blocked in Loose mode, please contact our technical support.

CC Protection When it's off, the following CC protection policies do not take effect

Cleansing Threshold ⓘ QPS

Set

步骤2：设置 CC 防护等级

1. 在 CC 防护开关和清洗阈值卡片中，单击**设置**，进入 CC 防护开关和清洗阈值规则列表。

For details about configuring domain name protection, contact your sales rep

CC Protection and Cleansing Threshold ⓘ

CC protection detects malicious behaviors according to access modes and connection status. In Loose Mode, only confirmed attack requests are blocked. In Medium mode, highly-suspicious requests are blocked. In Strict mode, all suspicious requests are blocked. If attack requests failed to be blocked in the Strict mode, or the normal requests are blocked in Loose mode, please contact our technical support.

CC Protection When it's off, the following CC protection policies do not take effect

Cleansing Threshold ⓘ QPS

Set

2. 在 CC 防护开关和清洗阈值规则列表中，单击左上角**新建**，选择绑定资源 IP 和所需的域名，设置防护状态及清洗阈值。

说明：

- 新建规则时域名项暂不支持泛域名输入
- 新建规则时，默认 CC 防护开关为打开状态。
- 清洗阈值为默认，业务刚接入的 DDoS 高防包实例的清洗阈值采用默认值，并随着接入业务流量的变化规律，系统自动学习形成一个基线值。并支持对单个域名维度进行清洗阈值自定义设置。

CC Protection and Cleansing Threshold
✕

Create

Associated Instance	Associated IP	Domain Name	Defense Status and Cleaning Threshold	Creation Time	Operation
by ■ ■ ■	Please select ▼		<input type="checkbox"/>		<div style="display: flex; gap: 5px;"> <div style="border: 1px solid #00aaff; padding: 2px 10px;">Save</div> <div style="border: 1px solid #ccc; padding: 2px 10px;">Cancel</div> </div>

Total items: 0
10 / page

⏪ ⏴ 1 / 1 page ⏵ ⏩

3. 单击**保存**，添加规则。

步骤3：设置精准防护策略

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. 在精准防护卡片中，单击**设置**，进入精准防护规则列表。

Block by location

Block requests to access Anti-DDoS Advanced instances from IP addresses in specified regions.

Configured 0 rules
Set

IP Blocklist/Allowlist

Configure IP blocklist and allowlist to block or allow requests from specific source IPs, so as to define who can access your application resource.

Configured 0 rules (max: 50 rules)
Set

Precise Protection

A protection policy with a combination of conditions of common HTTP fields

Configured 0 rules
Set

CC Frequency Limit

Set a limit to control to access frequency from the source IP.

Configured 0 rules
Set

2. 在精准防护规则列表中，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 高防包暂不支持 HTTPS 业务的精准防护配置，[DDoS 高防 IP](#) 可支持 HTTPS 业务的精准防护配置。

Create Precise Protection Policy ✕

Associate Service Packs **bgp-000001dc**

IP

Protocol HTTP

Domain Name

Match Condition

Field	Logic	Value	
uri	Equal to	<input type="text"/>	Delete
ua	Equal to	<input type="text"/>	Delete
cookie	Equal to	<input type="text"/>	Delete
referer	Equal to	<input type="text"/>	Delete
accept	Equal to	<input type="text"/>	Delete
srcip	Equal to	<input type="text"/>	Delete
Add			

Match Action

字段说明：

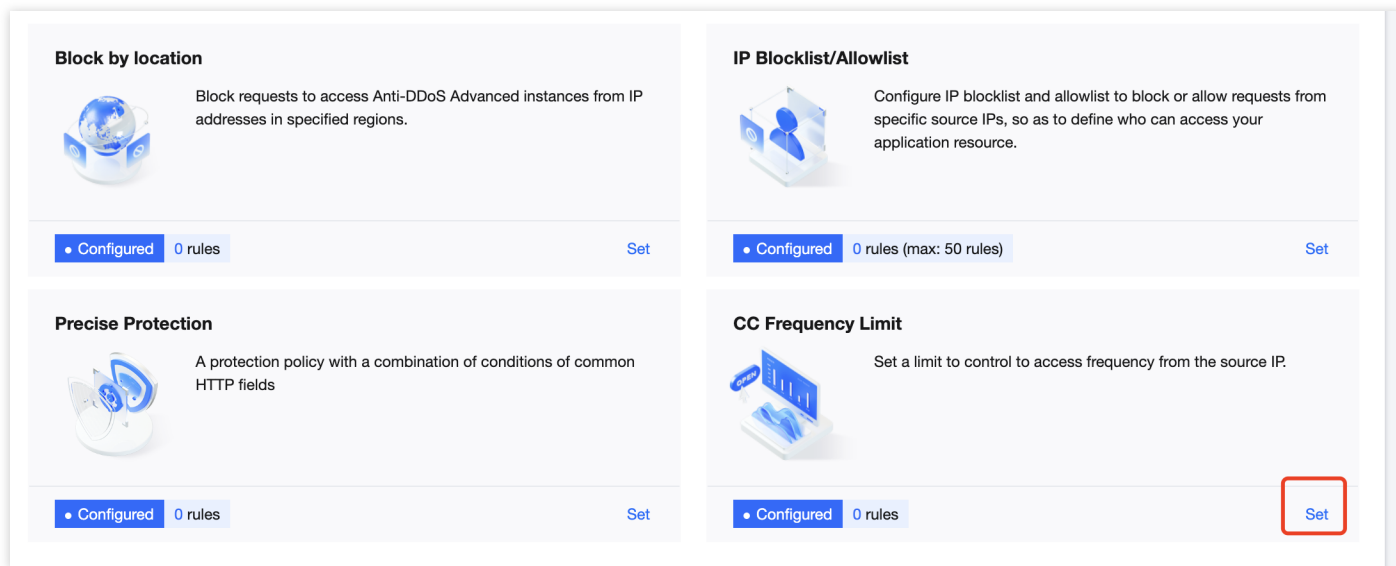
字段	字段描述
uri	访问请求的 URI 地址。

字段	字段描述
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。
匹配条件	人机校验和丢弃， <ul style="list-style-type: none"> • 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。 • 放行：对匹配条件直接通过。

步骤4：设置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。

1. 在右侧 CC 频率限制卡片中，单击**设置**，进入 CC 频率限制列表。



2. 在CC 频率限制列表中，可以新建防护等级，或对已创建的防护等级进行编辑。

说明：

防护等级为 DDoS 高防开启 CC 防护且遭受攻击触发清洗动作时，对流量检测的严格程度，分为五种等级：宽松、攻击紧急、适中、严格、自定义，可根据攻击情况进行选择，详细说明请参见 [CC 防护开关及清洗阈值](#)。

3. 单击**新建**，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 [频率控制](#)。

注意：

- 新增规则在自定义模式下才生效。
- 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。

CC Frequency R



Associate Service Packs **bgp-000001dc**

IP

Protocol HTTP

Domain Name

Field	Mode	Value
Add		

Frequency Limit Policy

Condition Every Seconds Access times ⓘ

Punishment time Seconds

OK

Cancel

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。
频率限制策略	人机校验和丢弃， <ul style="list-style-type: none">• 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。• 放行：对匹配条件直接通过。
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。

模拟 DDoS 攻击测试规则

最近更新时间：2022-08-29 10:59:43

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）

高防 EIP 创建使用指引

最近更新时间：2023-06-25 14:43:07

说明：

仅标准账号类型支持创建**高防 EIP**，若您无法确定账户类型。

步骤一：购买企业版高防包

登录腾讯云官网，进入 [DDoS 高防包购买页](#) 进行选购。更多详情请参见 [购买指引](#)。

步骤二：创建 BGP 带宽包

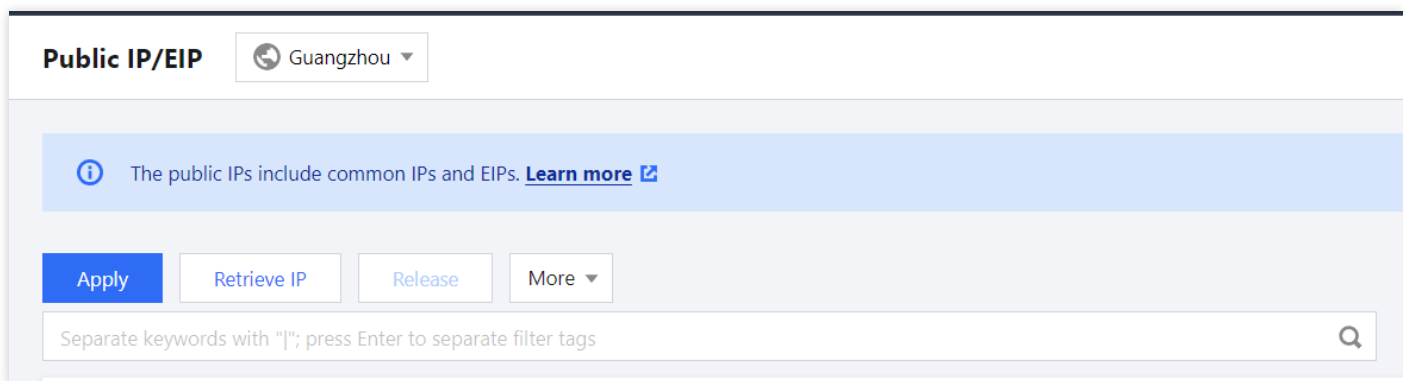
参考 [创建 IP 带宽包](#) 文档，创建 BGP 带宽包。

说明：

如您在需要使用的地域已创建常规 BGP 带宽包 可跳过此步骤至 [步骤三](#)。

步骤三：创建高防 EIP

1. 登录 [云服务器控制台](#)，在左侧操作栏中，单击**公网 IP**。
2. 在公网 IP 页面，选择地域，单击**申请**。



3. 在申请 EIP 窗口中，配置相关参数，单击**确定**，完成 EIP 的申请。

Apply for EIP ✕

IP address type

- General BGP IP
General BGP IP, balancing the network quality and costs.
- Accelerated IP Recommended
Anycast Acceleration, making public network access more stable, reliable and low latency
- Static single-line IP
Public network access through a single ISP is for the ease of independent scheduling at a low cost
- Anti-DDoS EIP New
Provide Tbps-level DDoS protection capability in combination with Anti-DDoS Pro for Enterprise. It cannot be switched to other address types.

Region

Central availability zone

South China (Guangzhou)

Billing mode ⓘ [Blurred]

Bandwidth cap - 1 + Mbps

Amount - 1 + 4/20

Name ⓘ

Tags ▶ Add

Public network fee [Blurred]

IP idle fees [Blurred]

Agreed to [Tencent Cloud EIP Service Level Agreement](#) and [Payment Overdue](#)

OK
Cancel

参数	说明
IP 地址类型	选择 高防 EIP

参数	说明
计费模式	无需选择，高防 EIP 仅支持共享带宽包计费模式
共享带宽包	选择需要加入的 常规 BGP 共享带宽包
带宽上限	请按需设置带宽上限，合理分配带宽资源
企业版高防包	选择需要绑定的 企业版高防包
数量	请按需选择申请的数量且确保 EIP 总数未超过产品总配额
名称	EIP 实例名称，非必填
标签	如需添加标签可在此进行添加，可通过标签进行权限管理

后续操作

若需要为 EIP 绑定云资源，请 [联系我们](#)。