DDoS 防护

最佳实践

产品文档

腾讯云

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
- 高防 EIP 创建使用指引
- CC 防护策略配置流程及注意事项
- 快速同步转发规则至新的高防 IP
- 通过智能调度实现三网流量调度

最佳实践
BGP 高防包异地防护方案

最近更新时间：2024-05-06 15:10:20

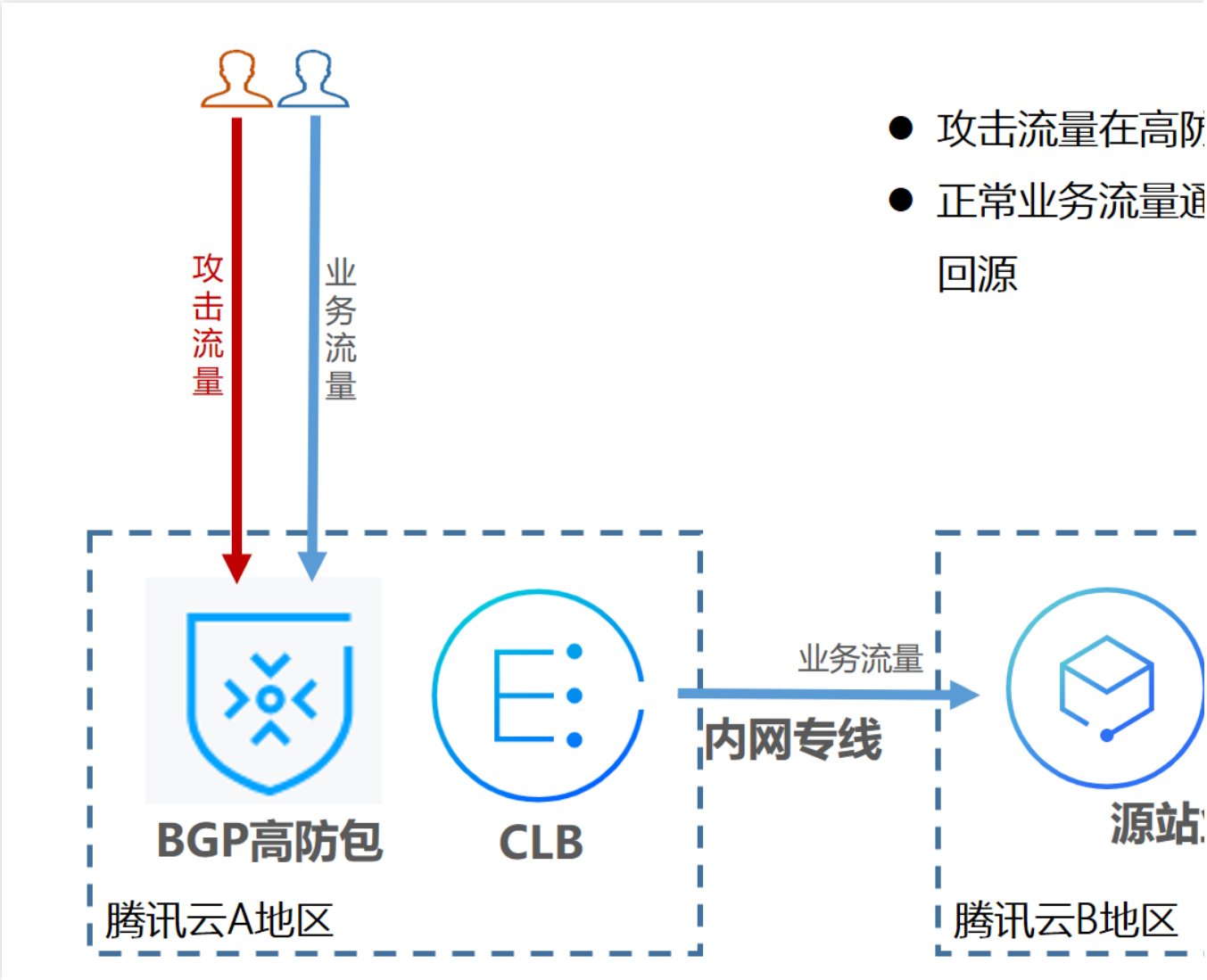
需求背景

受客观因素影响，DDoS 高防包仅支持腾讯云北京，上海，广州区域的用户，并承诺全力防护能力。全力防护指以成功防护每一次 DDoS 攻击为目标，整合当前本地清洗中心能力，同时会根据当时的实际网络状态进行动态调整，全力对攻击进行抵御。除此之外，中国大陆成都、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 高防包防护能力时，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 防护能力。
业务流量使用腾讯云的内网专线进行转发，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

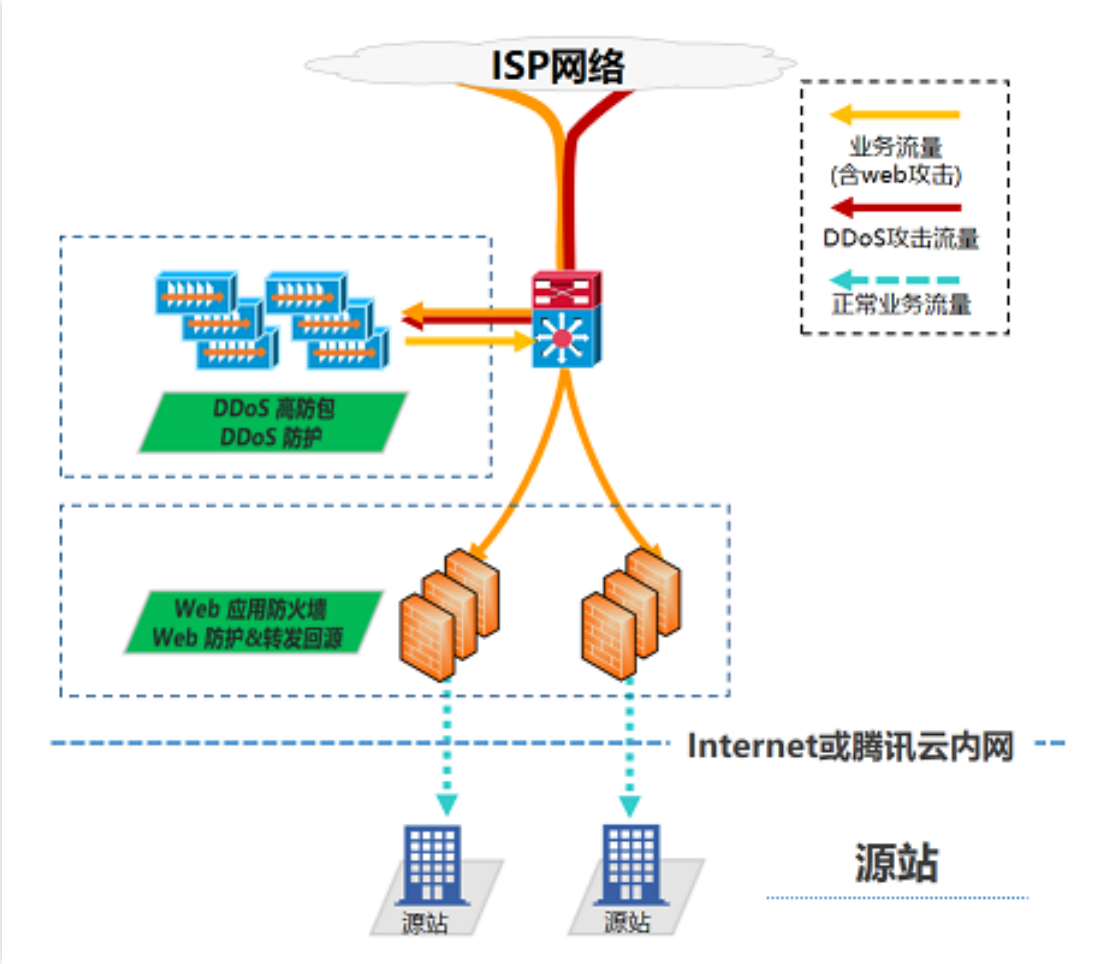
提前部署 DDoS 高防包和 CLB 负载均衡。
建立业务可用性监测机制，在未部署自动切换机制的情况下，发现源站访问异常及时介入处理。
定期进行验证和演练，了解和熟悉方案细节，解决可能存在的问题。

BGP 高防包与 Web 应用防火墙结合使用

最近更新时间：2024-05-06 15:10:20

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 防护（新版）控制台，在左侧导航中，单击**云上防护实例**。
2. 在云上防护实例页面，选择目标实例，单击操作列的**管理防护对象**。

3. 管理防护对象窗口中，根据实际防护需求选择“关联设备类型”及“资源实例”。

关联设备类型：支持云主机，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。

4. 选择完成后，单击**确定**即可。

业务系统压力测试建议

最近更新时间：2024-05-06 15:10:20

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：2024-05-06 15:10:20

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。

高防 EIP 创建使用指引

最近更新时间：2024-05-06 15:10:20

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，请联系我们。

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。


申请EIP
IP 地址类型
常规 BGP IP
普通线路 BGP IP，用于平衡网络质量与成本
加速 IP
推荐
采用 Anycast 加速，使公网访问更稳定、可靠、低延迟
静态单线 IP
通过单个网络运营商访问公网，成本低且便于自主调度
高防 EIP
new
配合企业版高防包，提供 Tbps 级别 DDos 全力防护，不支持转换为其他地址类型
所属地域
中心可用区
华南地区（广州）
计费模式
按流量
共享带宽包
带宽上限
20
40
60
100
1
Mbps
数量
1
您当前地域下已拥有 3 个 EIP，还可以申请 17 个EIP
名称
可选，不填默认未命名
高级选项
标签
公网网络费用
正在查询
IP资源费用
按流量计费和按共享带宽包计费的公网IP（包括普通公网IP和EIP），将按使用时长收取IP资源费。
同意《腾讯云EIP服务协议》、《欠费规则》
确定
取消

参数	说明

IP 地址类型	选择高防 EIP
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。

CC 防护策略配置流程及注意事项

最近更新时间：2024-05-06 15:10:20

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

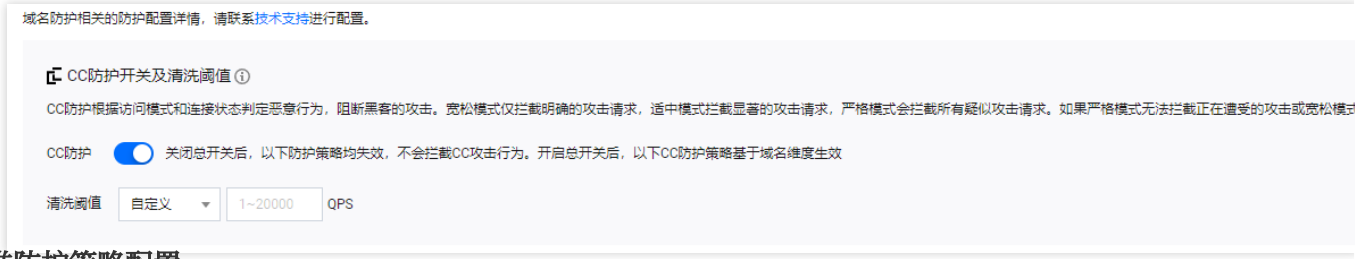
1. 登录 DDoS 防护（新版）控制台，在左侧导航中，单击**防护策略** > **CC 防护**。
2. 在左边的列表选中高防 IP 的 ID 下面的域名，如**212.64.xx.xx bgpip-000002je** > **http:80** > **www.xxx.com&quot**。

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。



4. **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。

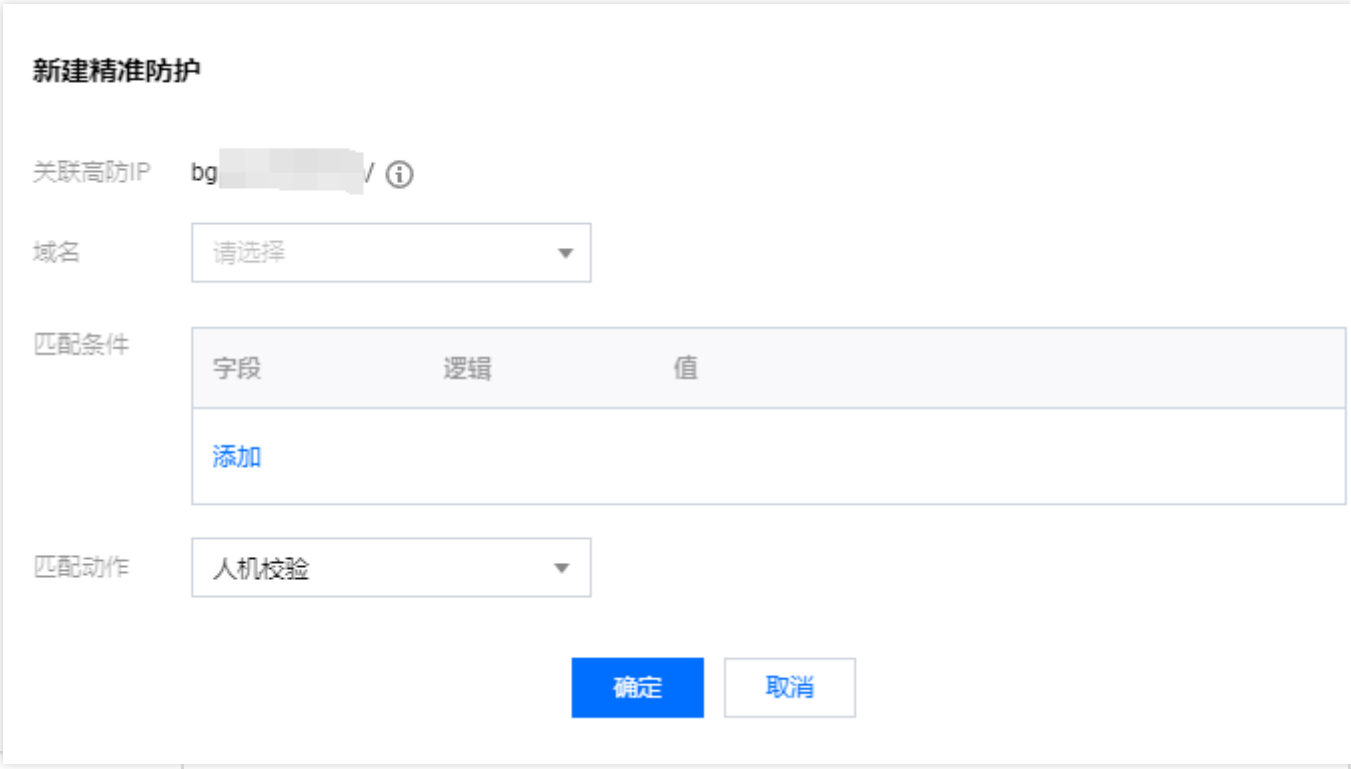
4.1 在精准防护卡片中，单击**设置**，进入频率限制规则列表。

4.2 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	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。
匹配动作	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。

5. **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。

5.1 在 CC 频率限制卡片中，单击**设置**，进入精准防护规则列表。

5.2 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 频率限制。

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。

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	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：2024-05-06 15:10:20

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 防护（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 输入栏中搜索 > 显示配置的转发规则 > 选择要导出的转发规则 > 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：2024-05-06 15:10:20

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。
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 防护 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 防护 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，例如腾讯云的 DNS 解析 DNSPod。

操作步骤

1. 登录 DDoS 防护（新版）控制台，在左侧导航栏中，单击**智能调度**。
2. 在智能调度页面，单击**新建调度**，系统自动生成一个 CNAME 记录。
3. 新建智能调度页面，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。
关于智能调度的配置，请参见 智能调度。