DDoS 高防 IP

快速入门

产品文档

腾讯云

文档目录

快速入门
网站业务接入

最近更新时间：2020-07-08 13:30:48

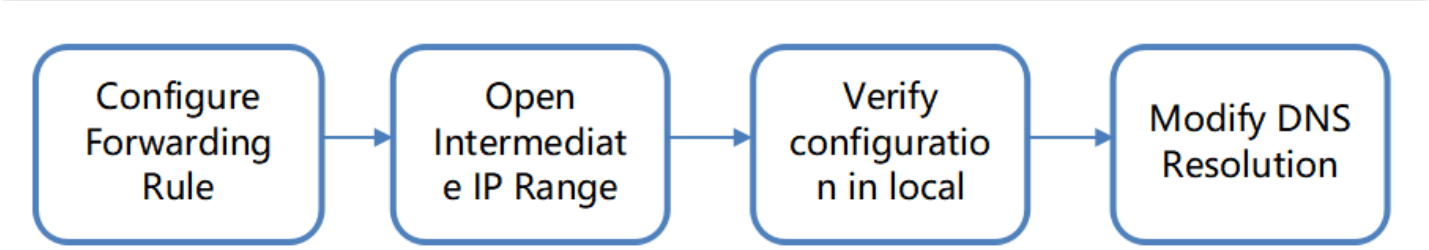
本文档介绍了网站类业务用户将业务接入 DDoS 高防 IP 实例并验证转发配置的详细操作步骤。

> 目前网站业务支持北京、上海、广州地区接入，暂不支持境外区域。

前提条件

- 在添加转发规则前，您需要成功购买 中国大陆 DDoS 高防 IP 实例 或 境外 DDoS 高防 IP 实例。
- 在修改业务域名 DNS 信息前，您需要成功购买域名解析产品。

操作流程

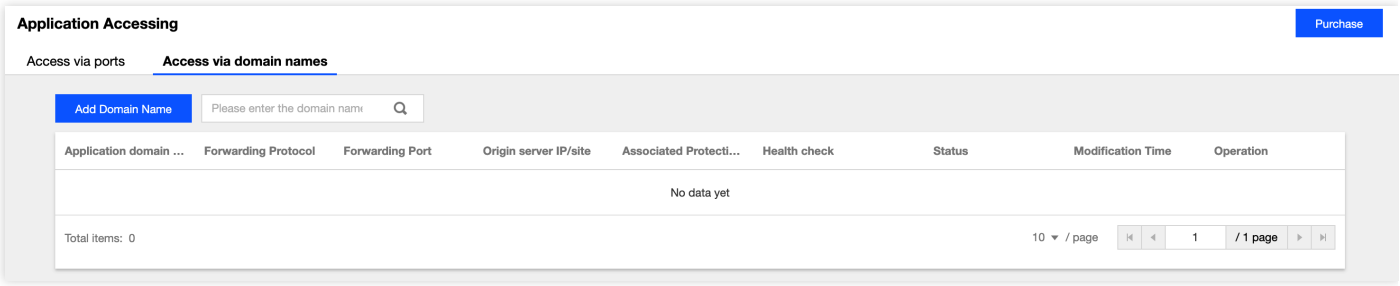


操作步骤

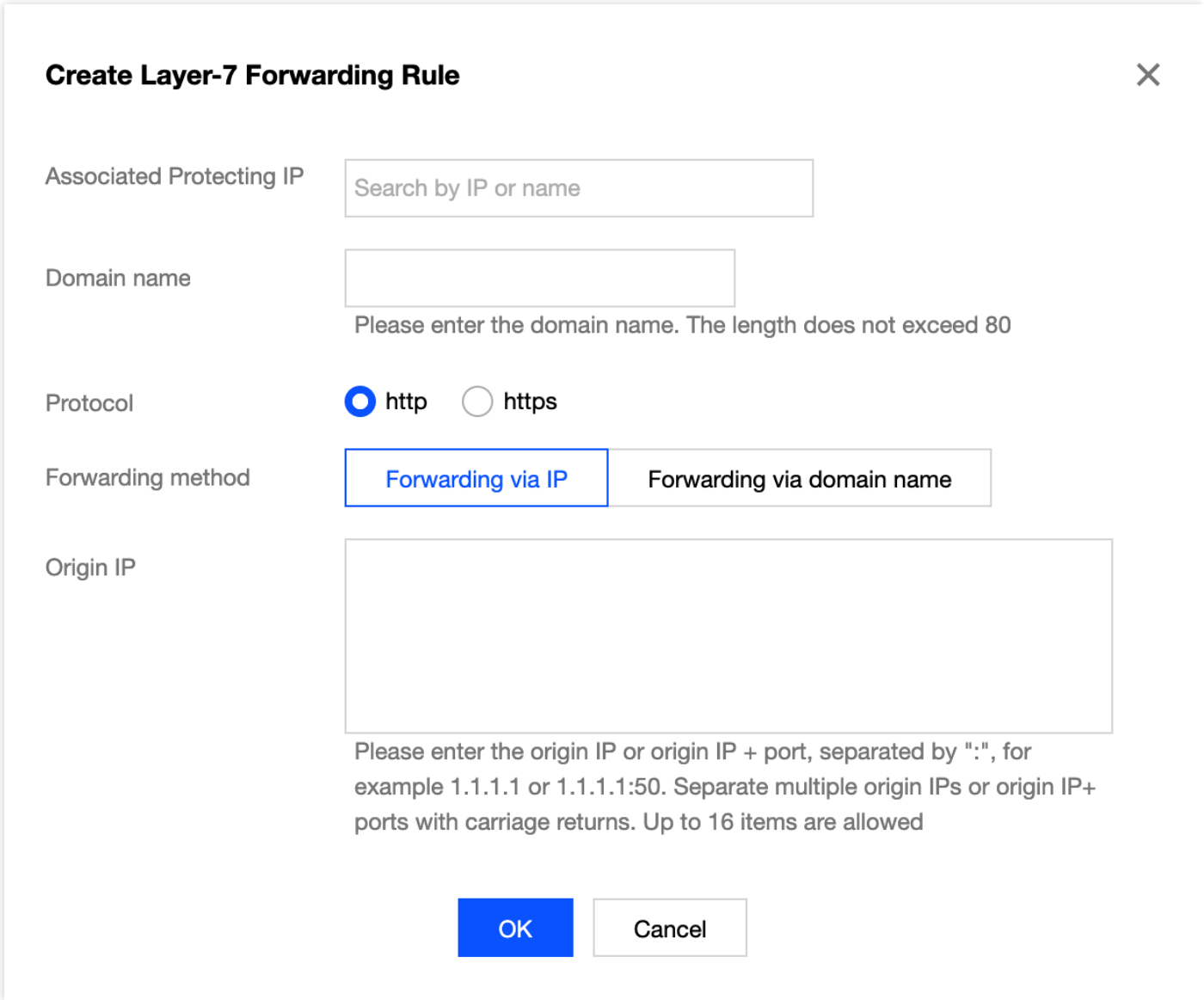
配置转发规则

1. 登录 DDoS 高防 IP（新版）管理控制台，在左侧导航栏单击【业务接入】。

2. 在“业务接入”页面，选择【域名接入】页签，单击【添加域名】。



3. 在添加转发规则页面中，根据实际需求配置如下参数。



参数说明：

- 域名：填写需要配置防护的网站域名。
- 协议：支持 HTTP 和 HTTPS，请根据实际业务需求勾选：

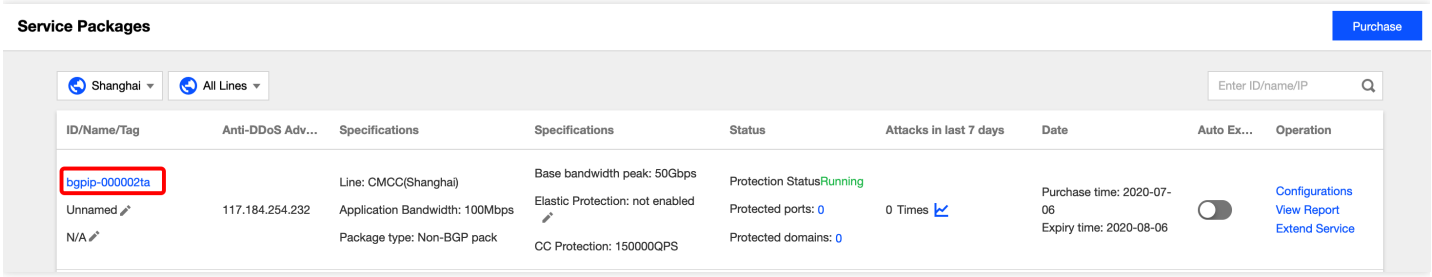
业务场景	相关操作
只包含 HTTP 协议的网站	勾选【HTTP】。
只包含 HTTPS 协议的网站	▪ 勾选【HTTPS】。 ▪ 证书来源：默认选择腾讯云托管证书。 ▪ 证书：选择对应的 SSL 证书名称。

- 回源方式支持【IP 回源】和【域名回源】
  - 若勾选【IP 回源】，则填写源站服务器的 IP （或 IP+端口）。一个网站域名对应多个源站 IP（或 IP+端口）时，可全部填入并用回车分隔多个 IP（或 IP+端口），最多支持填写16个 IP（或 IP+端口）。
  - 若勾选【域名回源】，则填写回源域名（CNAME）或域名（CNAME）+端口。一个网站域名对应多个源站域名（CNAME）或域名（CNAME）+端口时，可全部填入并用回车分隔多个域名（CNAME）或域名（CNAME）+端口，最多支持填写16个域名（CNAME）或域名（CNAME）+端口。

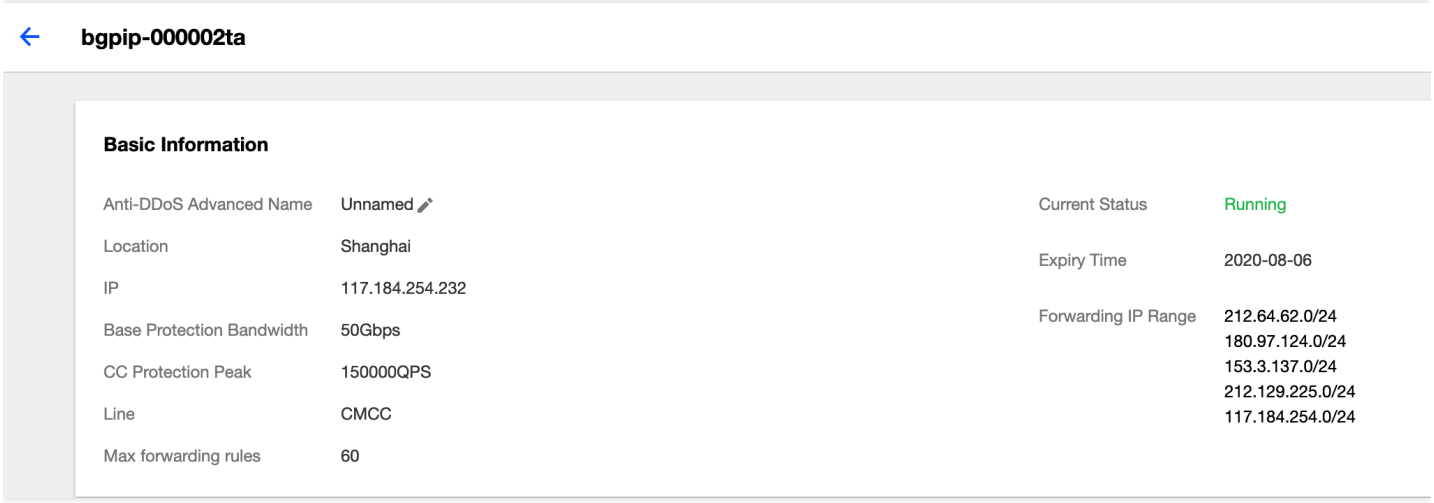
放行回源 IP 段

为了避免源站拦截 DDoS 高防 IP 的回源 IP 而影响业务，建议在源站的防火墙、Web 应用防火墙、IPS 入侵防护系统、流量管理等硬件设备上设置白名单策略，将源站的主机防火墙和其他任何安全类的软件（如安全狗等）的防护功能关闭或设置白名单策略，确保高防的回源 IP 不受源站安全策略的影响。

用户可以通过 DDoS 高防 IP（新版）管理控制台，在左侧导航栏，单击【实例列表】，找到对应实例 ID。



单击实例 ID 进入基本信息页面，查看高防 IP 回源段。



本地验证配置

转发配置完成后，DDoS 高防 IP 实例的高防 IP 将按照转发规则将相关端口的报文转发到源站的对应端口。
为了最大程度保证业务的稳定，建议在全面切换业务之前先进行本地测试。具体的验证方法如下：

1. 修改本地 hosts 文件，使本地对于被防护站点的请求经过高防。下面以 Windows 操作系统为配置本地hosts文件。
   打开本地计算机 `C:\Windows\System32\drivers\etc` 路径下的 hosts 文件，在文末添加如下内容：

   ```
   <高防 IP 地址> <被防护网站的域名>
   ```

   例如高防 IP 为10.1.1.1，域名为 `www.qqq.com` ，则添加：

   ```
   10.1.1.1 www.qqq.com
   ```

   保存 hosts 文件。在本地计算机对被防护的域名运行 ping 命令。当解析到的 IP 地址是 hosts 文件中绑定的高防 IP 地址时，说明本地hosts生效。

   > 若解析到的 IP 地址依然是源站地址，可尝试在 Windows 的命令提示符中运行 `ipconfig /flushdns` 命令刷新本地的 DNS 缓存。

2. 确认 hosts 绑定已经生效后，使用域名进行验证。若能正常访问则说明配置已经生效。

若使用正确的方法显示验证失败，请登录 DDoS 高防 IP 控制台检查配置是否正确。排除配置错误和验证方法不正确后，若问题依然存在，请 提交工单 联系我们协助。

非网站业务接入

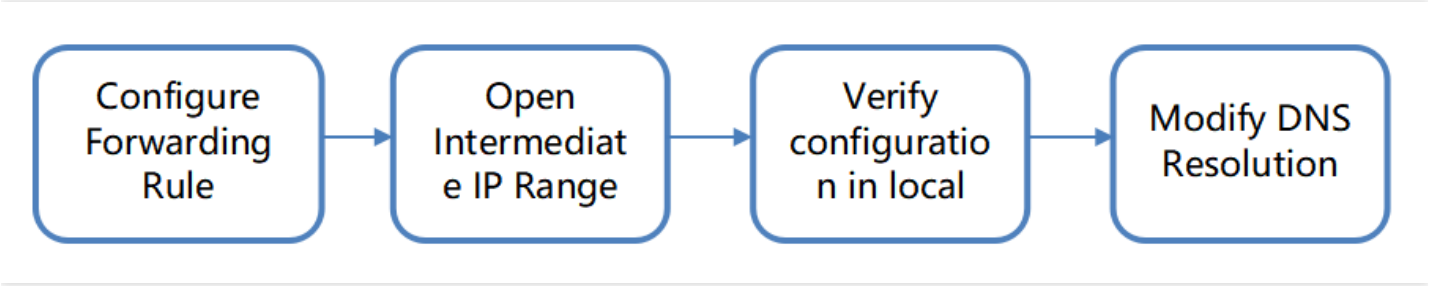
最近更新时间：2020-07-08 13:30:49

本文档介绍了非网站类业务用户如何将业务接入 DDoS 高防 IP 实例并验证转发配置。

前提条件

- 在添加转发规则前，您需要成功购买 中国大陆 DDoS 高防 IP 实例 或 境外 DDoS 高防 IP 实例。
- 在修改业务域名 DNS 信息前，您需要成功购买域名解析产品。

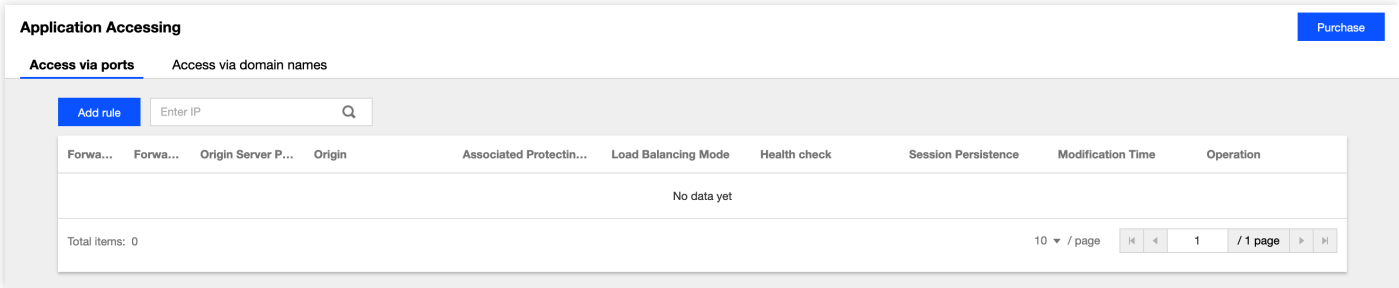
操作流程



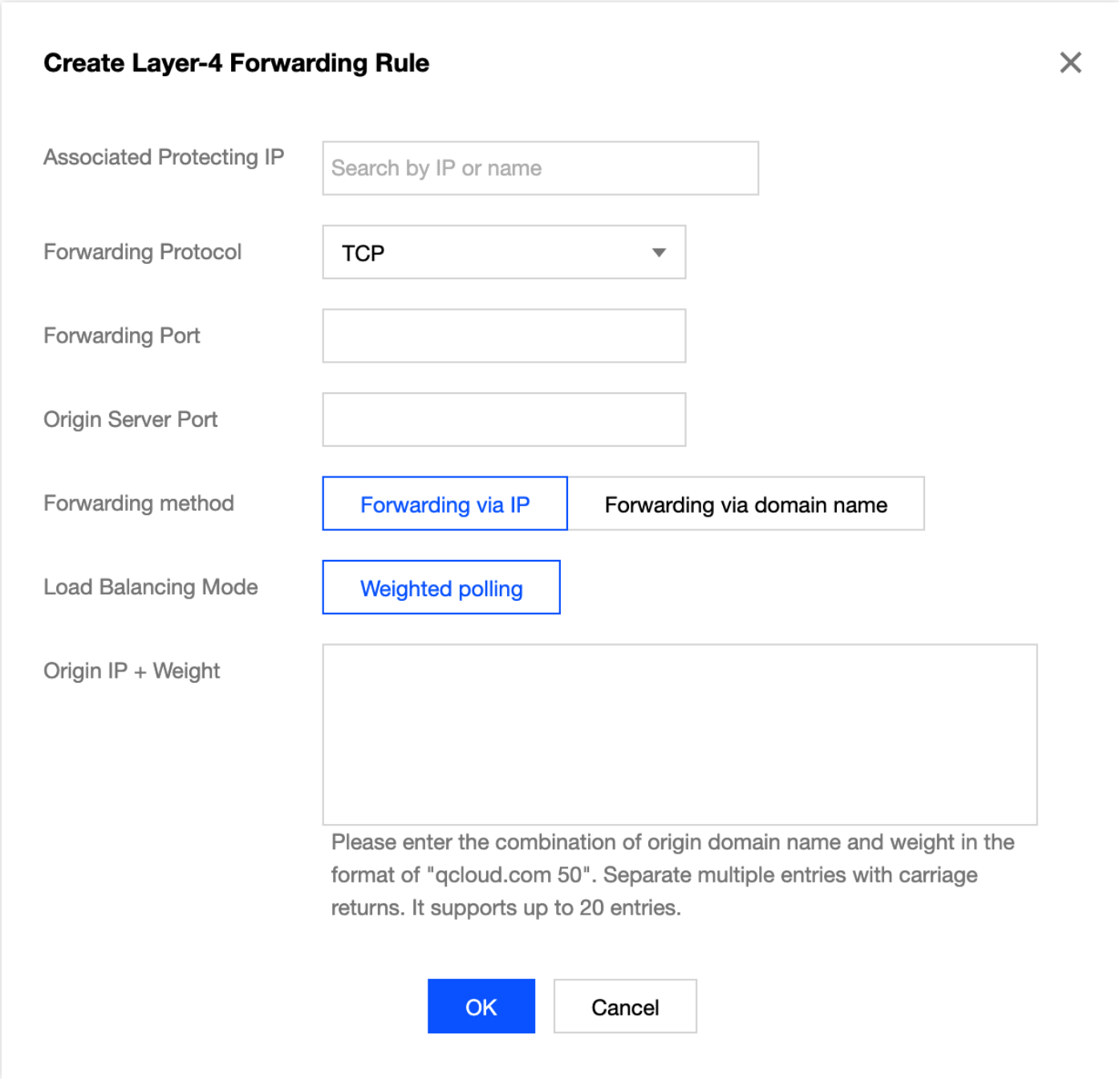
操作步骤

配置转发规则

1. 登录 DDoS 高防 IP（新版）管理控制台，在左侧导航栏，单击【业务接入】。
2. 在“业务接入”页面，选择【端口接入】页签，单击【添加规则】



3. 在添加转发规则页面中，根据实际需求配置如下参数。



参数说明：

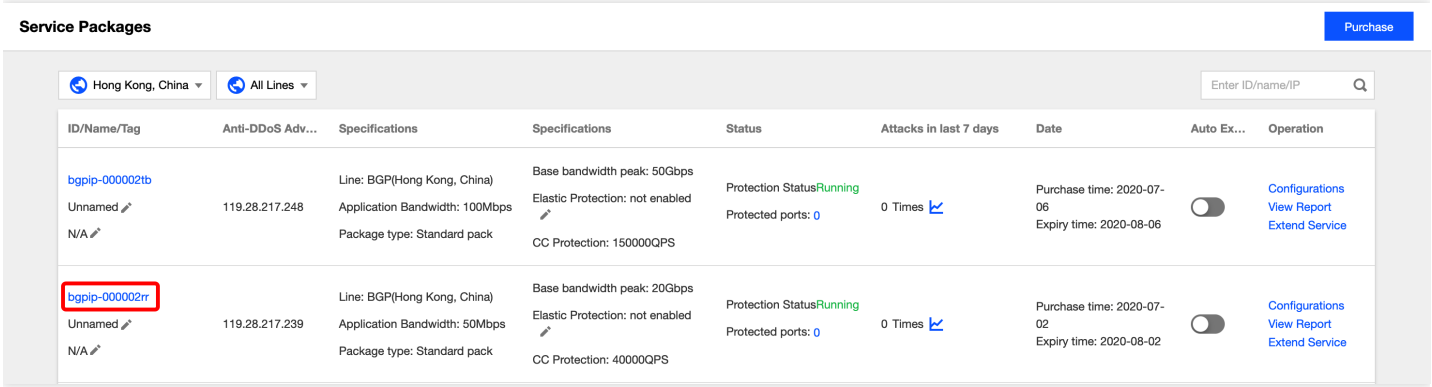
- 关联高防 IP：选择高防 IP。
- 转发协议：目前支持 TCP 和 UDP。
- 转发端口：用于访问的高防 IP 端口，建议选择跟源站相同端口。DDoS 高防 IP 除了北京、广州地区，其他地区不支持使用843端口为转发端口。
- 源站端口：用户业务站点的真实端口。
- 回源方式：支持 IP 回源和域名回源。
- 负载均衡方式：目前仅支持加权轮询。

- 源站IP+权重或源站域名。根据【回源方式】填写源站 IP + 权重或源站域名。最多支持20个 IP + 权重或域名。
  - 若勾选【IP 回源】，则填写源站服务器的 IP 地址 + 权重。一个域名对应多个源站 IP +权重时，可全部填入并用回车分隔多个 IP + 权重，最多支持20个。如1.1.1.1 50。
  - 若勾选【域名回源】，则填写回源域名。一个域名对应多个源站域名时，可全部填入并用回车分隔多个域名，最多支持20个。

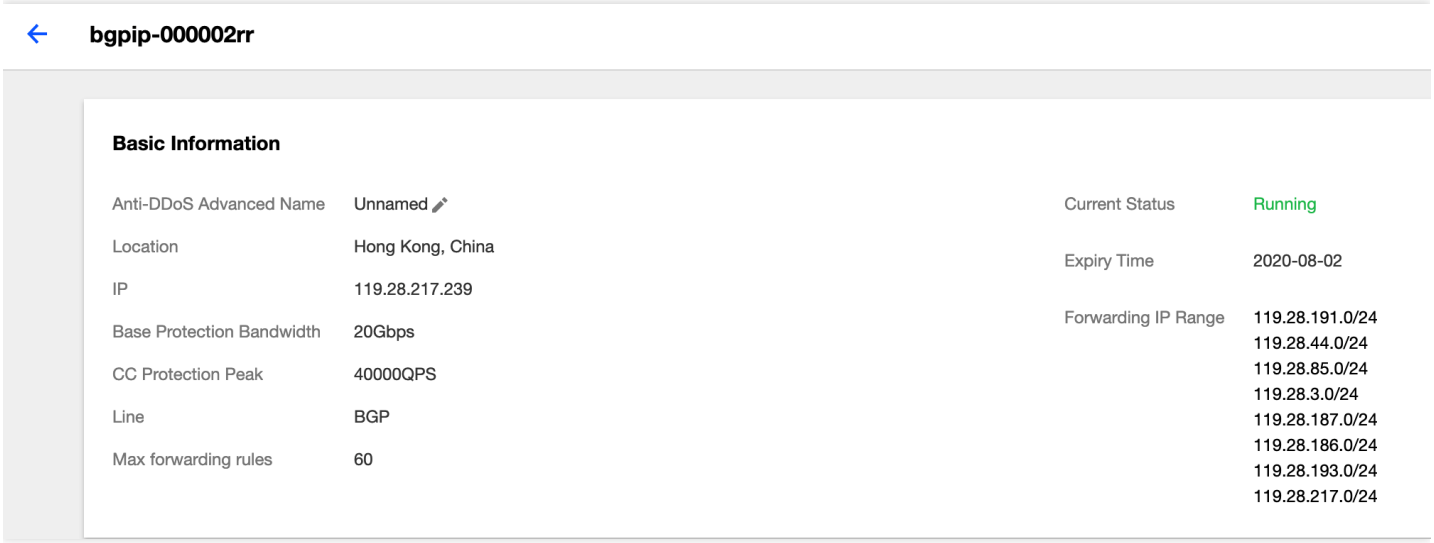
放行回源 IP 段

为了避免源站拦截 DDoS 高防 IP 的回源 IP 而影响业务，建议在源站的防火墙、Web 应用防火墙、IPS 入侵防护系统、流量管理等硬件设备上设置白名单策略，将源站的主机防火墙和其他任何安全类的软件（如安全狗等）的防护功能关闭或设置白名单策略，确保高防的回源 IP 不受源站安全策略的影响。

用户可以通过登录 DDoS 高防 IP（新版）管理控制台，在左侧导航栏中，单击【实例列表】，找到对应实例 ID。



单击实例 ID 进入基本信息页面，查看高防 IP 回源段。



本地验证配置

转发配置完成后，DDoS 高防 IP 实例的高防 IP 将按照转发规则将相关端口的报文转发到源站的对应端口。
为了最大程度保证业务的稳定，建议在全面切换业务之前先进行本地测试。具体的验证方法如下：

- **使用 IP 访问的业务**
  对于直接通过 IP 进行交互的业务（如游戏业务），可通过 `telnet` 命令访问高防 IP 端口，查看是否能连通。
  若能在本地客户端直接填写服务器 IP，则直接填入高防 IP 进行测试，查看本地客户端是否可以正常连接。

  例如高防 IP 为10.1.1.1，转发端口为1234，源站 IP 为10.2.2.2，源站端口为1234。本地通过 `telnet` 命令访问 10.1.1.1:1234，`telnet` 命令能连通则说明转发成功。

- **使用域名访问的业务**
  对于需要通过域名访问的业务，可通过修改本地hosts来验证配置是否生效。
  a. 修改本地 hosts 文件，使本地对于被防护站点的请求经过高防。下面以 Windows 操作系统为配置本地hosts文件。
  打开本地计算机 `C:\Windows\System32\drivers\etc` 路径下的 hosts 文件，在文末添加如下内容：

  ```
  <高防 IP 地址> <被防护网站的域名>
  ```

  例如高防 IP 为10.1.1.1，域名为 `www.qqq.com` ，则添加：

  ```
  10.1.1.1 www.qqq.com
  ```

  保存 hosts 文件。在本地计算机对被防护的域名运行 ping 命令。当解析到的 IP 地址是 hosts 文件中绑定的高防 IP 地址时，说明本地 hosts 生效。

  > 若解析到的 IP 地址依然是源站地址，可尝试在 Windows 的命令提示符中运行 `ipconfig /flushdns` 命令刷新本地的 DNS 缓存。

  b. 确认 hosts 绑定已经生效后，使用域名进行验证。若能正常访问则说明配置已经生效。

> 若使用正确的方法仍验证失败，请登录 DDoS 高防 IP 控制台检查配置是否正确。排除配置错误和验证方法不正确后，若问题依然存在，请联系 腾讯云技术支持 。