DDoS 高防 IP 专业版

快速入门

产品文档

腾讯云

文档目录

快速入门
非网站业务接入

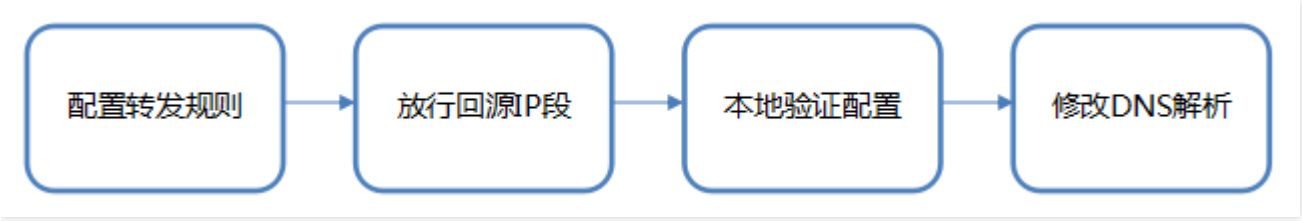
最近更新时间：2019-12-23 15:41:54

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 专业版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 DDoS 高防 IP 专业版实例。
- 在修改业务域名 DNS 信息前，您需要成功购买域名解析产品，例如腾讯云的 云解析。

操作流程



操作步骤

配置转发规则

1. 登录 DDoS 防护（大禹）管理控制台，选择【高防IP专业版】>【接入配置】。

2. 在【非网站业务】页签，查找并选择目标 DDoS 高防 IP 专业版实例，单击【添加规则】。

3. 根据实际需求配置如下参数，单击【确认】。

- 业务域名：填写业务域名信息。该项用于说明该条规则对应的业务域名，便于规则识别与管理，报表统计。
- 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 专业版不支持使用843、1433、1434、3306、3389、36000以及56000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 专业版的回源 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 防护（大禹）管理控制台，在左侧导航栏选择【高防 IP 专业版】>【防护配置】，在防护配置页面单击【防护策略】，在“防护信息”区域查看详细的高防 IP 回源地址段。

本地验证配置

转发配置完成后，DDoS 高防 IP 专业版实例包含的5个高防 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对5个高防 IP 全部进行本地测试。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，可通过以下的方法来验证配置是否生效：

  i. 修改本地 hosts 文件，使本地对于被防护站点的请求经过高防。
  以Windows操作系统为例：

  a. 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.qq.com ，则添加：
  `10.1.1.1 www.qq.com`
  b. 保存 hosts 文件。

  ii. 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，说明转发成功。

  > 说明：
  > 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。

  iii. 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。

> 说明：

若使用正确的方法仍验证失败，请登录 DDoS 防护（大禹）管理控制台 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 。

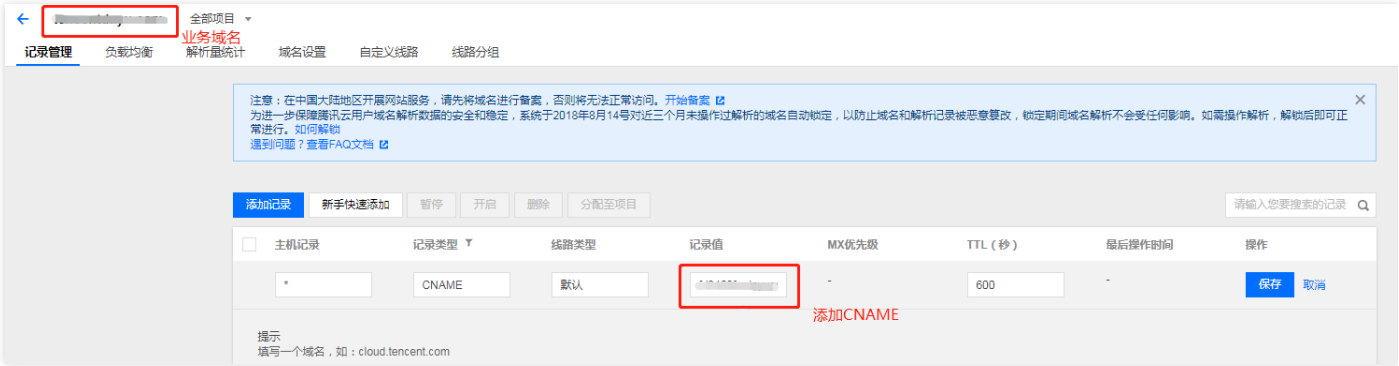
修改业务域名 DNS 解析

使用 DDoS 高防 IP 专业版防护前，需要将业务域名 DNS 的 CNAME 记录修改为 DDoS 高防 IP 专业版实例的 CNAME，使所有用户访问网站的流量都先经过 DDoS 高防 IP 再回到源站（即先将所有流量都牵引到 DDoS 高防 IP 再回到源站）。

说明：
不同域名解析产品的配置原理相同，具体配置步骤可能有细微差别，本文以使用腾讯云域名解析产品为例。

1. 登录 腾讯云控制台，选择【云产品】>【域名与网站】>【云解析】，在【域名解析列表】中，单击目标域名所在行的【解析】。

2. 在域名记录管理页签，单击【添加记录】，记录类型选择 CNAME，记录值内输入 DDoS 高防 IP 专业版自动生成的 CNAME 地址，单击【保存】。



3. 修改完成后，待 DNS 记录生效，DDoS 高防 IP 专业版即可对访问网站的流量进行防护。

网站业务接入

最近更新时间：2019-12-23 15:41:59

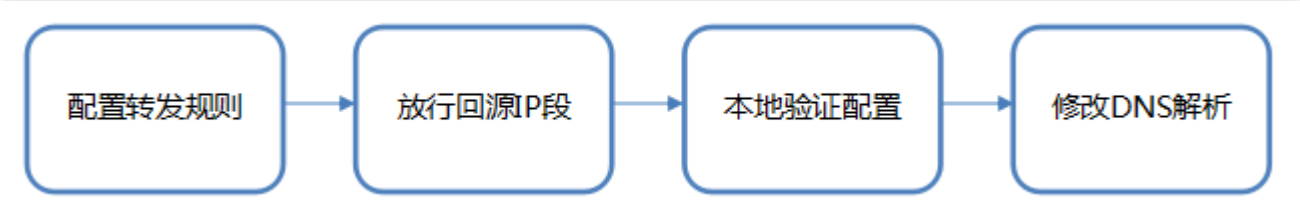
本文档介绍了网站类业务用户将业务接入 DDoS 高防 IP 专业版实例并验证转发配置的详细操作步骤。

> 注意：
> 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 DDoS 高防 IP 专业版实例。
- 在修改业务域名 DNS 信息前，您需要成功购买域名解析产品，例如腾讯云的 云解析。

操作流程

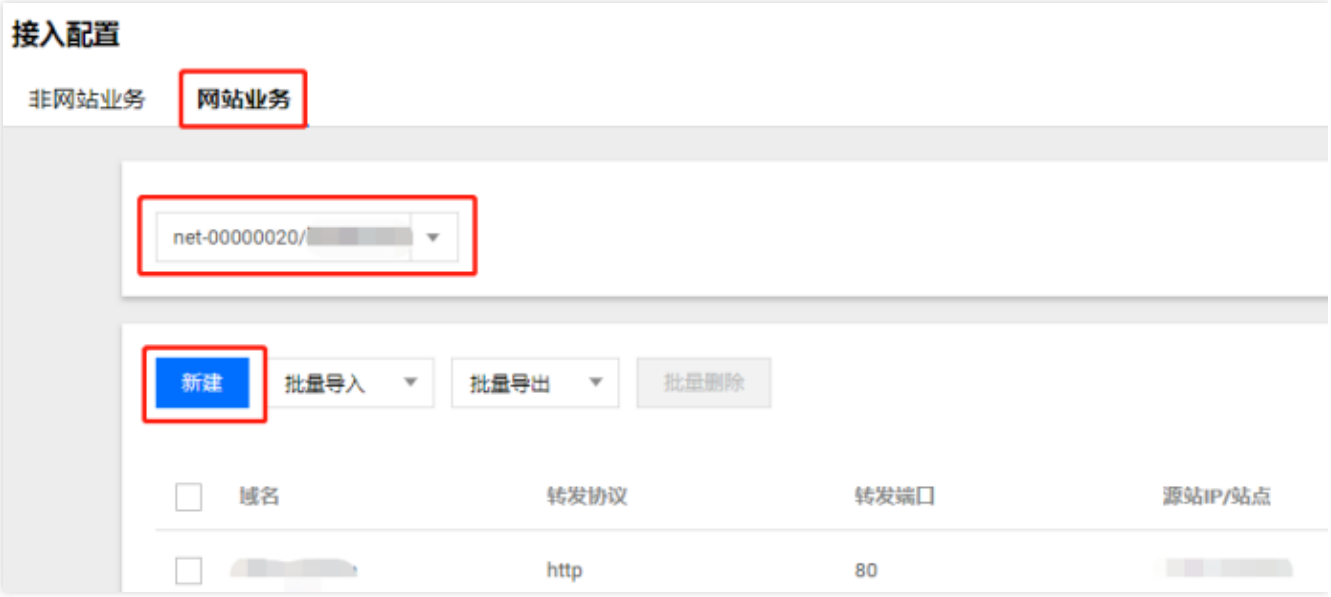


操作步骤

配置转发规则

1. 登录 DDoS 防护管理控制台，在左侧导航栏选择【DDoS 高防 IP 专业版】>【接入配置】。
2. 在接入配置页面，单击【网站业务】，查找并选择目标 DDoS 高防 IP 专业版实例，添加转发规则。
   - 单个添加转发规则：

a. 单击【新建】。


接入配置
非网站业务
网站业务
net-00000020/
新建
批量导入
批量导出
批量删除
域名
转发协议
转发端口
源站IP/站点
http
80

b. 在添加转发规则页面中，根据实际需求配置如下参数，单击【确定】。

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。

- 根据【回源方式】填写源站 IP 或源站域名：
  - 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。

- 批量添加转发规则：

  a. 选择【批量导入】>【导入转发规则】。

b. 在批量导入页面的规则输入框中，粘贴需要导入的规则

注意：

- 粘贴内容从左至右依次是域名、协议、源站 IP（暂不支持源站域名）、源站端口。源站 IP 与源站端口之间以英文":"分隔，其它的中间由空格分隔。一行只能填写一条转发规则。
- 批量添加的转发规则条目数不允许超过当前配额。

放行回源 IP 段

为了避免源站拦截 DDoS 高防 IP 专业版的回源 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 防护管理控制台，在左侧导航栏选择【DDoS 高防 IP 专业版】>【防护配置】，进入防护配置页面，单击【防护策略】，在服务包信息区域查看所使用 DDoS 高防 IP 专业版实例的详细高防 IP 回源地址段。

本地验证配置

转发配置完成后，DDoS 高防 IP 专业版实例包含的5个高防 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对5个高防 IP 进行本地验证。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。
   以 Windows 操作系统为例：
   i. 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.qq.com` ，则添加：

   ```
   10.1.1.1 www.qq.com
   ```

   ii. 保存 hosts 文件。
2. 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，说明转发成功。

> 说明：
> 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。

3. 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。

> 说明：
> 若使用正确的方法显示验证失败，请登录 DDoS 防护管理控制台 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 。

修改业务域名 DNS 解析

使用 DDoS 高防 IP 专业版防护前，需要将业务域名 DNS 的 CNAME 记录修改为 DDoS 高防 IP 专业版实例的 CNAME，使所有用户访问网站的流量都先经过高防 IP 再回到源站（即先将所有流量都牵引到高防 IP 再回到源站）。

> 说明：
> 不同域名解析产品的配置原理相同，具体配置步骤可能有细微差别，本文以使用腾讯云域名解析产品为例。

1. 登录 腾讯云控制台，选择【云产品】>【域名与网站】>【云解析】，在【域名解析列表】中，单击目标域名所在行的操作【解析】。

2. 在域名记录管理页签，单击【添加记录】，记录类型选择 CNAME，记录值内输入 DDoS 高防 IP 专业版自动生成的 CNAME 地址，单击【保存】。