

DDoS 高防 IP

快速入门

产品文档



腾讯云

【版权声明】

©2013-2019 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

快速入门

网站业务接入

非网站业务接入

快速入门

网站业务接入

最近更新时间：2020-07-08 13:30:48

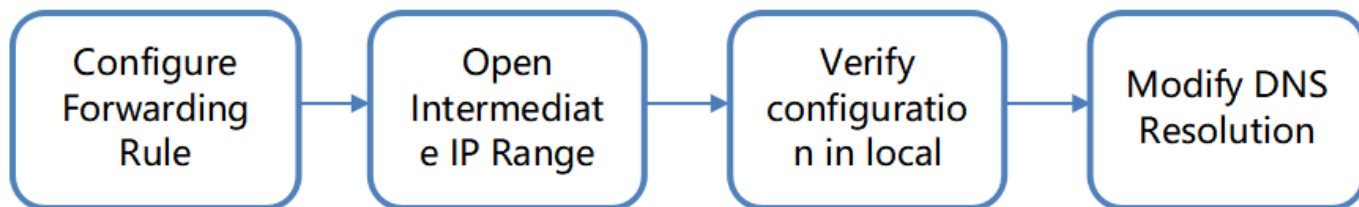
本文档介绍了网站类业务用户将业务接入 DDoS 高防 IP 实例并验证转发配置的操作步骤。

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

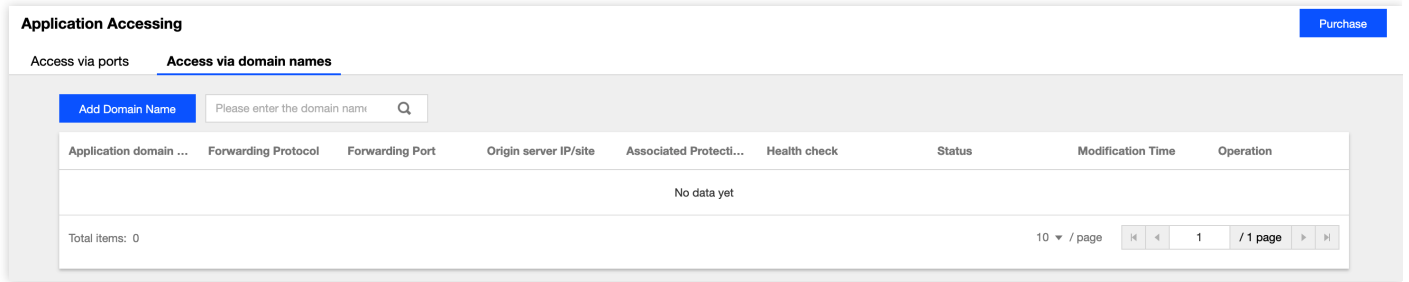


操作步骤

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。

Create Layer-7 Forwarding Rule ✕

Associated Protecting IP

Domain name
Please enter the domain name. The length does not exceed 80

Protocol http https

Forwarding method

Origin IP
Please enter the origin IP or origin IP + port, separated by ":", for example 1.1.1.1 or 1.1.1.1:50. Separate multiple origin IPs or origin IP+ ports with carriage returns. Up to 16 items are allowed

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	<ul style="list-style-type: none"> 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。

Service Packages Purchase

Shanghai All Lines Enter ID/name/IP

ID/Name/Tag	Anti-DDoS Adv...	Specifications	Specifications	Status	Attacks in last 7 days	Date	Auto Ex...	Operation
bgpip-000002ta	117.184.254.232	Line: CMCC(Shanghai) Application Bandwidth: 100Mbps	Base bandwidth peak: 50Gbps Elastic Protection: not enabled CC Protection: 150000QPS	Protection StatusRunning Protected ports: 0 Protected domains: 0	0 Times	Purchase time: 2020-07-06 Expiry time: 2020-08-06	<input type="checkbox"/>	Configurations View Report Extend Service
Unnamed								
N/A		Package type: Non-BGP pack						

单击实例 ID 进入基本信息页面，查看高防 IP 回源段。

← bgpip-000002ta

Basic Information

Anti-DDoS Advanced Name	Unnamed ✎	Current Status	Running
Location	Shanghai	Expiry Time	2020-08-06
IP	117.184.254.232	Forwarding IP Range	212.64.62.0/24 180.97.124.0/24 153.3.137.0/24 212.129.225.0/24 117.184.254.0/24
Base Protection Bandwidth	50Gbps		
CC Protection Peak	150000QPS		
Line	CMCC		
Max forwarding rules	60		

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.qq.com`，则添加：

```
10.1.1.1 www.qq.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

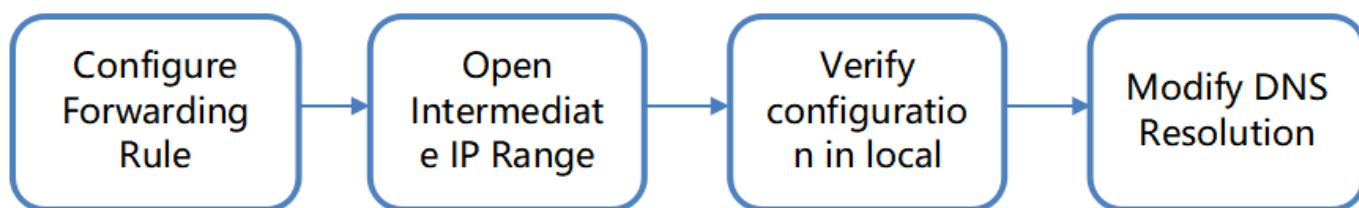
最近更新时间：2020-07-08 13:30:49

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。

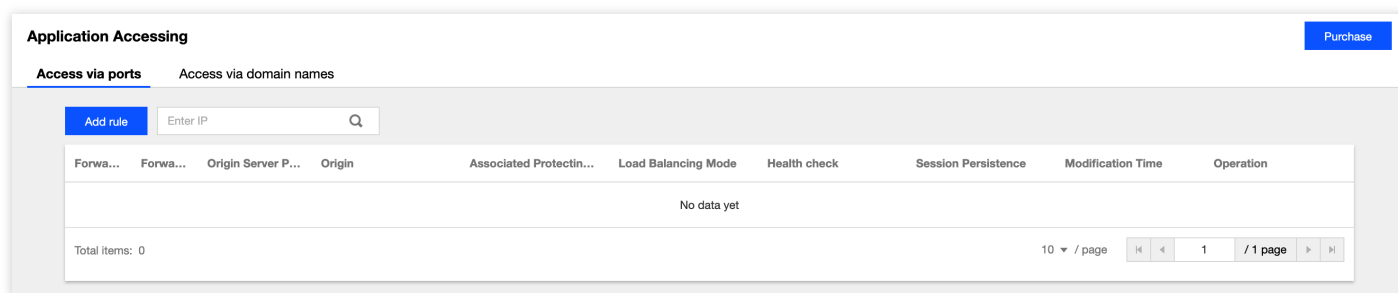
操作流程



操作步骤

配置转发规则

- 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】。
- 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。

Create Layer-4 Forwarding Rule ✕

Associated Protecting IP

Forwarding Protocol

Forwarding Port

Origin Server Port

Forwarding method

Load Balancing Mode

Origin IP + Weight

Please enter the combination of origin domain name and weight in the format of "qcloud.com 50". Separate multiple entries with carriage returns. It supports up to 20 entries.

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。

ID/Name/Tag	Anti-DDoS Adv...	Specifications	Specifications	Status	Attacks in last 7 days	Date	Auto Ex...	Operation
bgpip-000002tb Unnamed N/A	119.28.217.248	Line: BGP(Hong Kong, China) Application Bandwidth: 100Mbps Package type: Standard pack	Base bandwidth peak: 50Gbps Elastic Protection: not enabled CC Protection: 150000QPS	Protection StatusRunning Protected ports: 0	0 Times	Purchase time: 2020-07-06 Expiry time: 2020-08-06	<input type="checkbox"/>	Configurations View Report Extend Service
bgpip-000002rr Unnamed N/A	119.28.217.239	Line: BGP(Hong Kong, China) Application Bandwidth: 50Mbps Package type: Standard pack	Base bandwidth peak: 20Gbps Elastic Protection: not enabled CC Protection: 40000QPS	Protection StatusRunning Protected ports: 0	0 Times	Purchase time: 2020-07-02 Expiry time: 2020-08-02	<input type="checkbox"/>	Configurations View Report Extend Service

单击实例 ID 进入基本信息页面，查看高防 IP 回源段。

Basic Information		Current Status	Running
Anti-DDoS Advanced Name	Unnamed	Expiry Time	2020-08-02
Location	Hong Kong, China	Forwarding IP Range	119.28.191.0/24 119.28.44.0/24 119.28.85.0/24 119.28.3.0/24 119.28.187.0/24 119.28.186.0/24 119.28.193.0/24 119.28.217.0/24
IP	119.28.217.239		
Base Protection Bandwidth	20Gbps		
CC Protection Peak	40000QPS		
Line	BGP		
Max forwarding rules	60		

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.qq.com`，则添加：

```
10.1.1.1 www.qq.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](#)。