

DDoS 高防 IP

快速入门

产品文档



腾讯云

【版权声明】

©2013-2020 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

接入非网站业务

接入网站业务

快速入门

接入非网站业务

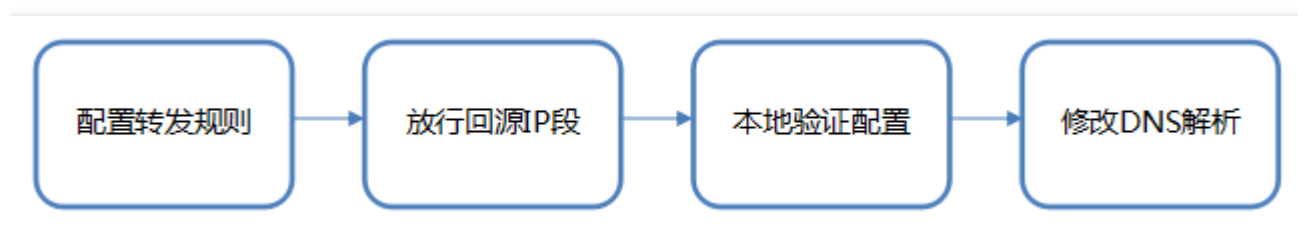
最近更新时间：2020-03-30 17:07:46

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 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，例如腾讯云的 [DNS 解析 DNSPod](#)。

操作流程



操作步骤

配置转发规则

- 登录 [DDoS 防护管理控制台](#)，选择【DDoS 高防 IP】>【接入配置】。
- 在【非网站业务】页签，查找并选择目标 DDoS 高防 IP 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

腾讯云基于态势感知SSA提供永久免费的云安全统一管理平台，方便用户全局化管理云安全风险、安全事件，并获取威胁情报及安全大屏展示能力，开始使用态势感知SSA

华南地区(广州)

BGP

bgpip-000001y6/

新建

批量导入批量导出批量删除

☐	转发协议/端口	源站端口	源站IP/域名	负载均衡方式	健康检查	会话保持
☐	TCP/4430	443	47	加权轮询	开启 编辑	关闭 编辑

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】。

添加转发规则

转发协议

TCP

转发端口

源站端口

回源方式

IP回源

域名回源

负载均衡方式

加权轮询

源站IP + 权重

请用回车分隔多个IP + 权重，最多可输入本IP转发目标区域内20个公网IP + 权重，例如：1.1.1.1 50

确定

取消

- 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。

说明：

DDoS 高防 IP 不支持使用1433、1434、3306、3389、36000以及56000端口，广州、北京地区的支持843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。

说明：

权重的取值范围为1~100。

- 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。
- 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。

批量导入

规则

示例：TCP 1234 4321 1.1.1.1 10或TCP 1234 4321 a.com
注意：粘贴内容从左至右依次为协议、转发端口、源站端口、回源IP和权重（或回源域名），中间由空格分隔。一行只能填写一条转发规则。

确定取消

注意：

- 粘贴内容从左至右依次是转发协议、转发端口、源站端口、源站 IP、权重（或回源域名），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。在配额限制内，单次最大导入条目为30条。

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 防护管理控制台](#)，在左侧导航栏选择【DDoS 高防 IP】>【资产列表】，找到目标 DDoS 高防 IP 实例所在行，单击“ID/名称”，在弹出的“基础信息”页面中查看详细的高防 IP 回源地址段。

本地验证配置

转发配置完成后，DDoS 高防 IP 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 防护前，需要将业务域名 DNS 的 A 记录更换为高防 IP 地址，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 [DNS 解析 DNSPod 控制台](#)，在【域名解析列表】中，单击目标域名所在行的【解析】。

☐	域名	解析状态 ①	解析套餐	最后操作时间	操作
☐	s[REDACTED]	域名 DNS 未修改 ①	免费套餐	2017-08-31 12:19:41	解析 升级套餐 更多 ▼
☐	[REDACTED]	域名 DNS 未修改 ①	免费套餐	2017-08-30 20:34:34	解析 升级套餐 更多 ▼
☐	[REDACTED]	域名 DNS 未修改 ①	免费套餐	2017-07-22 21:57:15	解析 升级套餐 更多 ▼

2. 在域名记录管理页签，单击【添加记录】，将 A 记录指向的 IP 地址修改为 DDoS 高防 IP，单击【保存】。

← [REDACTED] 全部项目 ▼

记录管理 负载均衡 解析量统计 域名设置 自定义线路 线路分组

主域名

注意：在中国大陆地区开展网站服务，请先将域名进行备案，否则将无法正常访问。 [开始备案](#)
为进一步保障腾讯云用户域名解析数据的安全和稳定，系统于2018年8月14号对近三个月未操作过解析的域名自动锁定，以防止域名和解析记录被恶意篡改，锁定期间域名解析不会受任何影响。如需操作解析，解锁后即可正常进行。 [如何解锁](#)
遇到问题？查看FAQ文档 [FAQ文档](#)

添加记录 新手快速添加 暂停 开启 删除 分配至项目 请输入您要搜索的记录 Q

☐	主机记录	记录类型 ▼	线路类型	记录值	MX优先级	TTL (秒)	最后操作时间	操作
☐	p[REDACTED]	A	默认	1 [REDACTED]	-	600	-	保存 取消

提示
要解析 www.tencentdayu.com，请填写 www。主机记录就是域名前缀，常见用法有：

www	解析后的域名为 www.tencentdayu.com
@	直接解析主域名 tencentdayu.com
*	泛解析，匹配其他所有域名 *.tencentdayu.com
mail	将域名解析为 mail.tencentdayu.com，通常用于解析邮箱服务器
二级域名	如：abc.tencentdayu.com，填写abc
手机网站	如：m.tencentdayu.com，填写m

高防 IP

接入网站业务

最近更新时间：2020-03-30 17:06:11

本文档介绍了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。

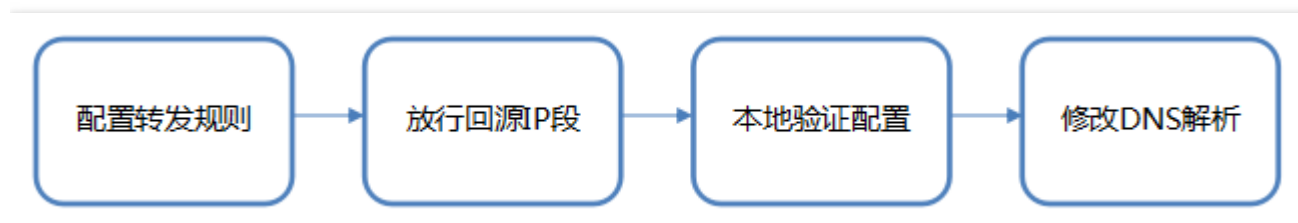
说明：

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 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 [DNS 解析 DNSPod](#)。

操作流程



操作步骤

配置转发规则

- 登录 [DDoS 防护管理控制台](#)，在左侧导航栏选择【DDoS 高防 IP】>【接入配置】。
- 在接入配置页面，单击【网站业务】，查找并选择目标 DDoS 高防 IP 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

腾讯云基于态势感知SSA提供永久免费的云安全统一管理平台，方便用户全局化管理云安全风险、安全事件，并获取威胁情报及安全

华南地区(广州)

BGP

bgpip-000001yn/

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	47.

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】。

添加转发规则

×

域名

请输入域名，长度不超过80

协议

☐ HTTP
☒ HTTPS

证书来源

腾讯云托管证书([SSL证书管理](#))

证书

请选择证书

回源方式

☒ IP 回源
☐ 域名回源

源站IP

请输入源站IP或源站IP+端口，后者中间用英文":"分隔，例如1.1.1.1或1.1.1.1:50。用回车分隔多个源站IP或源站IP+端口，最多支持16个

确定

取消

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】。

接入配置

非网站业务**网站业务**

华南地区(广州)BGPbgpip-0000020n/

新建

批量导入

批量导出

批量删除

☐ 域名

导入转发规则

导入健康检查

转发协议

转发端口

☐

https

443

b. 在批量导入页面的规则输入框中，粘贴需要导入的规则

批量导入

规则

a.com https 2.3.2.5:443 2.2.2.2:443

示例：a.com https 2.3.2.5:443 2.2.2.2:443

注意：以上字段含义从左至右依次为**域名**、**协议**、**源站IP(暂不支持源站域名)**、**源站端口**，即本示例的含义是添加一条规则，域名为**a.com**，协议类型为**https**，源站IP和端口包含两条：**2.3.2.5:443 2.2.2.2:443**。

确定

取消

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 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】>【资产列表】，找到目标 DDoS 高防 IP 实例所在行，单击“ID/名称”，在弹出的“基础信息”页面中查看详细的高防 IP 回源地址段。

本地验证配置

转发配置完成后，DDoS 高防 IP 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。

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：

若使用正确的方法仍验证失败，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 防护前，需要将业务域名 DNS 的 A 记录更换为高防 IP 地址，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 [DNS 解析 DNSPod 控制台](#)，在【域名解析列表】中，单击目标域名所在行的【解析】。

☐	域名	解析状态 ①	解析套餐	最后操作时间	操作
☐	s	域名 DNS 未修改 ①	免费套餐	2017-08-31 12:19:41	解析 升级套餐 更多
☐		域名 DNS 未修改 ①	免费套餐	2017-08-30 20:34:34	解析 升级套餐 更多
☐		域名 DNS 未修改 ①	免费套餐	2017-07-22 21:57:15	解析 升级套餐 更多

2. 在域名记录管理页签，单击【添加记录】，将 A 记录指向的 IP 地址修改为 DDoS 高防 IP，单击【保存】。

