

DDoS 防护

历史文档（高防包、高防 IP）



腾讯云

【 版权声明 】

©2013–2026 腾讯云版权所有

本文档（含所有文字、数据、图片等内容）完整的著作权归腾讯云计算（北京）有限责任公司单独所有，未经腾讯云事先明确书面许可，任何主体不得以任何形式复制、修改、使用、抄袭、传播本文档全部或部分内容。前述行为构成对腾讯云著作权的侵犯，腾讯云将依法采取措施追究法律责任。

【 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。未经腾讯云及有关权利人书面许可，任何主体不得以任何方式对前述商标进行使用、复制、修改、传播、抄录等行为，否则将构成对腾讯云及有关权利人商标权的侵犯，腾讯云将依法采取措施追究法律责任。

【 服务声明 】

本文档意在向您介绍腾讯云全部或部分产品、服务的当时的相关概况，部分产品、服务的内容可能不时有所调整。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默示的承诺或保证。

【 联系我们 】

我们致力于为您提供个性化的售前购买咨询服务，及相应的技术售后服务，任何问题请联系 4009100100或 95716。

文档目录

历史文档（高防包、高防 IP）

实践教程

- 遭受攻击后如何向网监报案
- 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
- 平滑切换线上业务至 DDoS 高防 IP
- 获取客户端真实 IP（端口接入）
- 获取客户端真实 IP（域名接入）
- 与源站结合的防护调度方案
- 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
- 云服务器被封堵后快速恢复业务
- 轻量应用服务器封堵后快速恢复业务

故障处理

- 配置安全组阻止入站后，仍遭受到 DDoS 攻击
- 公网 IP 遭遇 DDoS 攻击
- 业务被大流量攻击导致封堵
- DDoS 攻击未达到阈值业务 IP 被封堵
- 使用高防 IP，业务访问出现502报错
- 域名接入高防 IP，提示未备案

SDK 文档

- 水印 SDK
- 水印 SDK 个人信息保护规则

DDoS 高防包（旧版）

产品简介

- 产品概述
- 产品优势
- 应用场景
- 相关概念
- 相关产品

购买指南

计费概述

购买指引

续费指引

欠费说明

退费说明

快速入门

操作指南

操作总览

使用限制

实例管理

查看实例详情

设置资源名称

配置弹性防护

管理防护对象 IP

解封防护 IP

防护配置

配置清洗阈值与防护等级

配置业务场景

管理 DDoS 高级防护策略

配置 CC 防护策略

配置智能调度

配置攻击告警阈值

查看统计报表

查看操作日志

设置安全事件通知

实践教程

DDoS 高防包与 Web 应用防火墙结合使用

DDoS 高防包异地防护方案

业务系统压力测试建议

SDK 文档

水印 SDK

常见问题

封堵相关问题

功能相关问题

计费相关问题

DDoS 高防 IP（旧版）

产品简介

产品概述

- 产品优势
- 应用场景
- 相关概念
- 购买指南
 - 计费概述
 - 购买指引
 - 续费指引
 - 调整规格费用说明
 - 欠费说明
 - 退费说明
- 快速入门
 - 接入非网站业务
 - 接入网站业务
- 操作指南
 - 操作总览
 - 使用限制
 - 实例管理
 - 查看实例详情
 - 设置资源名称
 - 配置弹性防护
 - 调整 DDoS 高防 IP 实例规格
 - 解封防护 IP
 - 防护配置
 - 配置业务场景
 - 配置清洗阈值与防护等级
 - 管理 DDoS 高级防护策略
 - 配置 CC 防护等级
 - 管理 CC 防护策略
 - 配置健康检查
 - 配置会话保持
 - 配置智能调度
 - 配置攻击告警阈值
 - 查看统计报表
 - 查看操作日志
 - 设置安全事件通知
- 实践教程
 - 平滑切换线上业务至 DDoS 高防 IP
 - 源站 IP 暴露的解决方法

获取客户端真实 IP（域名接入）

与源站结合的防护调度方案

业务系统压力测试建议

SDK 文档

水印 SDK

常见问题

封堵相关问题

功能相关问题

计费相关问题

历史文档（高防包、高防 IP）

实践教学

遭受攻击后如何向网监报案

最近更新时间：2024-04-18 15:48:53

当业务遭受 DDoS 网络攻击时，推荐在采用 DDoS 高防服务来保障您的业务安全与稳定的同时，建议向网监部门进行报案。

报案流程

1. 遭受攻击后，应尽快向当地网监部门进行报案，并根据网监部门要求提供相关信息。
2. 网监部门判断是否符合立案标准，并进入网监处理流程。
3. 正式立案后，腾讯云会配合网监部门接口人提供攻击取证。

① 说明：

具体立案标准可向当地的网监部门进行咨询。

腾讯云能提供什么相关证据？

您的报案在网监部门立案后，腾讯云将配合网监部门提供以下协助：

- 腾讯云会配合网监部门，向网监接口人提供您在腾讯云平台上的业务的流量日志、遭受攻击信息等。

① 说明：

由于相关数据将作为法律证据，因此无法直接提供给您。您可以在腾讯云管理控制台中自行查看攻击流量的相关信息。

- 腾讯云不能对流量日志和攻击信息等进行分析，直接给出谁是攻击者的结论。

① 说明：

由于腾讯云不是法官，无法判定谁有罪；也不是具有执法权的警察，能够进行立案调查；腾讯云只能作为证据的提供者和证人。

- 腾讯云会及时响应网监部门的协助调查要求，配合开展工作。
- 建议您在遭受安全攻击时，参考当地网监部门的立案调查标准，积极请求公安网警进行立案调查。

查看攻击相关信息

您可以在 [DDoS 防护（新版）控制台](#) 查看流量、攻击事件、抓包信息等。

BGP 高防包异地防护方案

最近更新时间：2025-08-07 17:59:42

需求背景

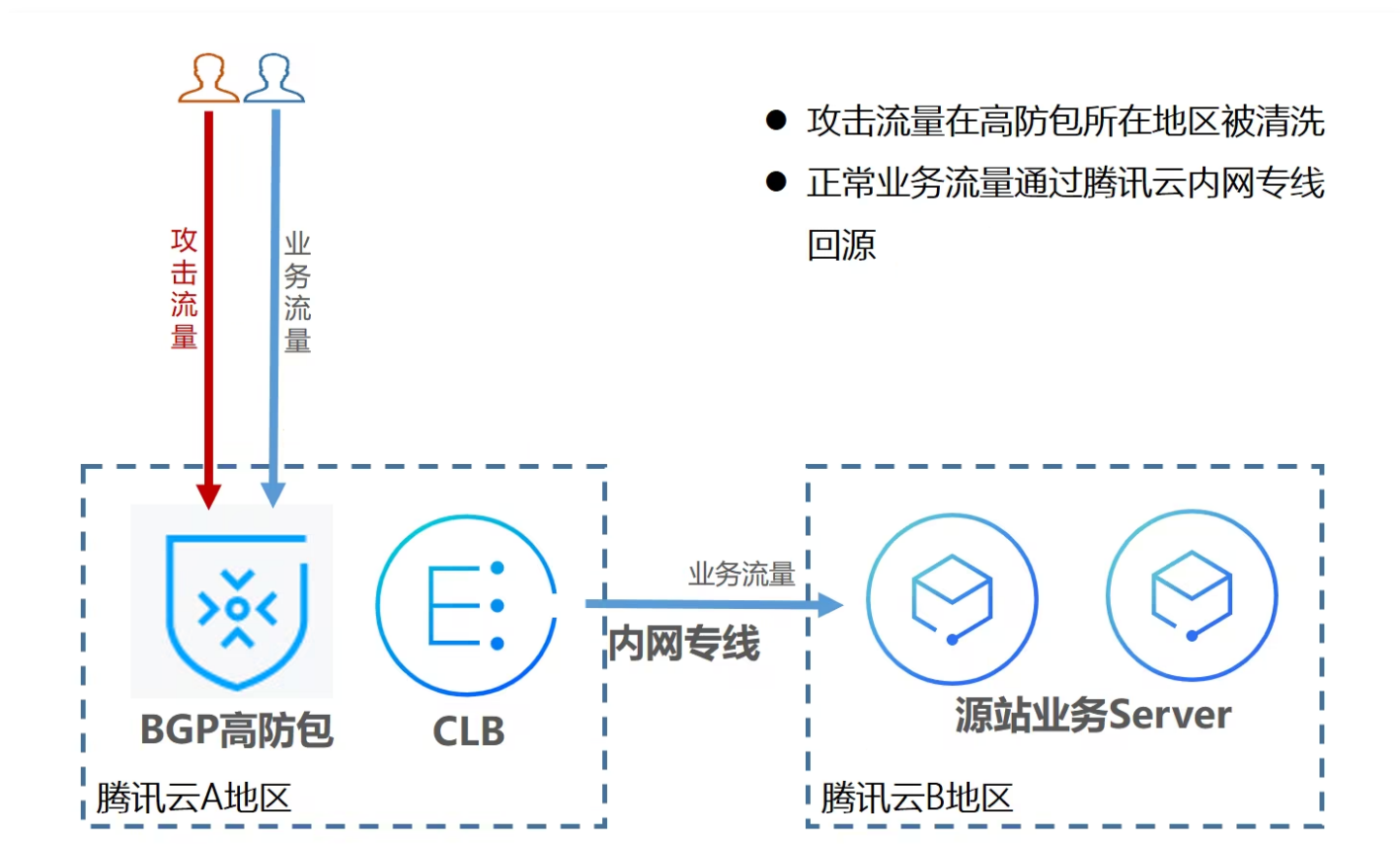
受客观因素影响，DDoS 高防包仅支持腾讯云北京，上海，广州区域的用户，并承诺全力防护能力。全力防护指以成功防护每一次 DDoS 攻击为目标，整合当前本地清洗中心能力，同时会根据当时的实际网络状态进行动态调整，全力对攻击进行抵御。除此之外，中国大陆成都、重庆等区域尚未上线高防包产品。如果用户业务源站部署在腾讯云，并且需要使用腾讯云非源站所在地区的 DDoS 高防包防护能力时，可参考本方案。

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300Gbps的 DDoS 防护能力。
- 业务流量使用腾讯云的内地网专线进行转发，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。

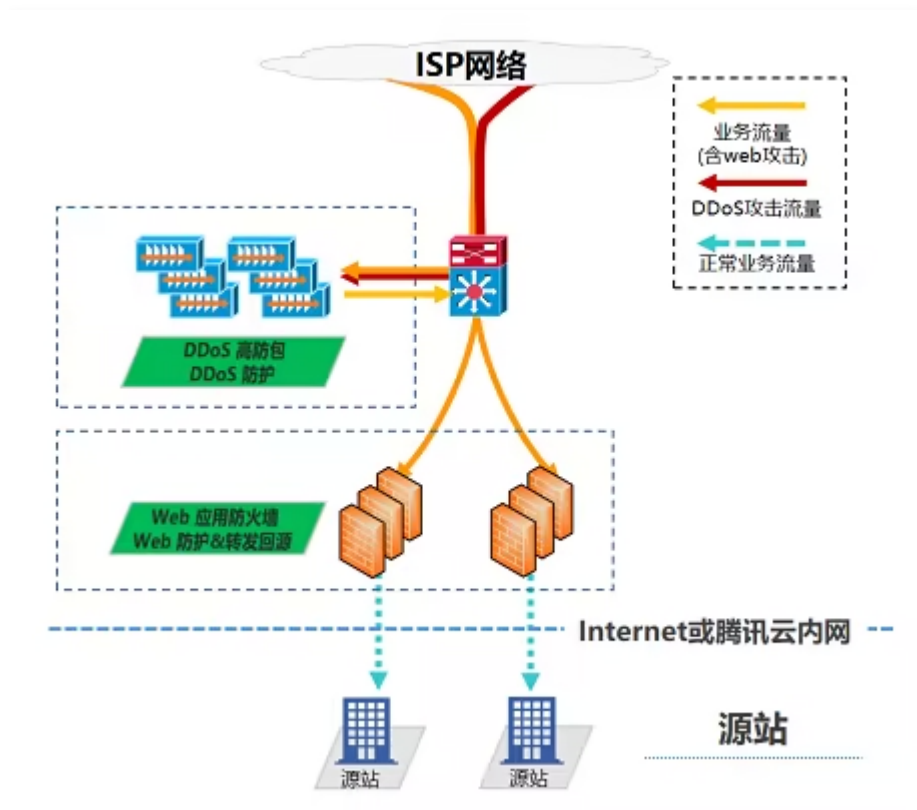
BGP 高防包与 Web 应用防火墙结合使用

最近更新时间：2026-01-28 14:44:46

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](#)。

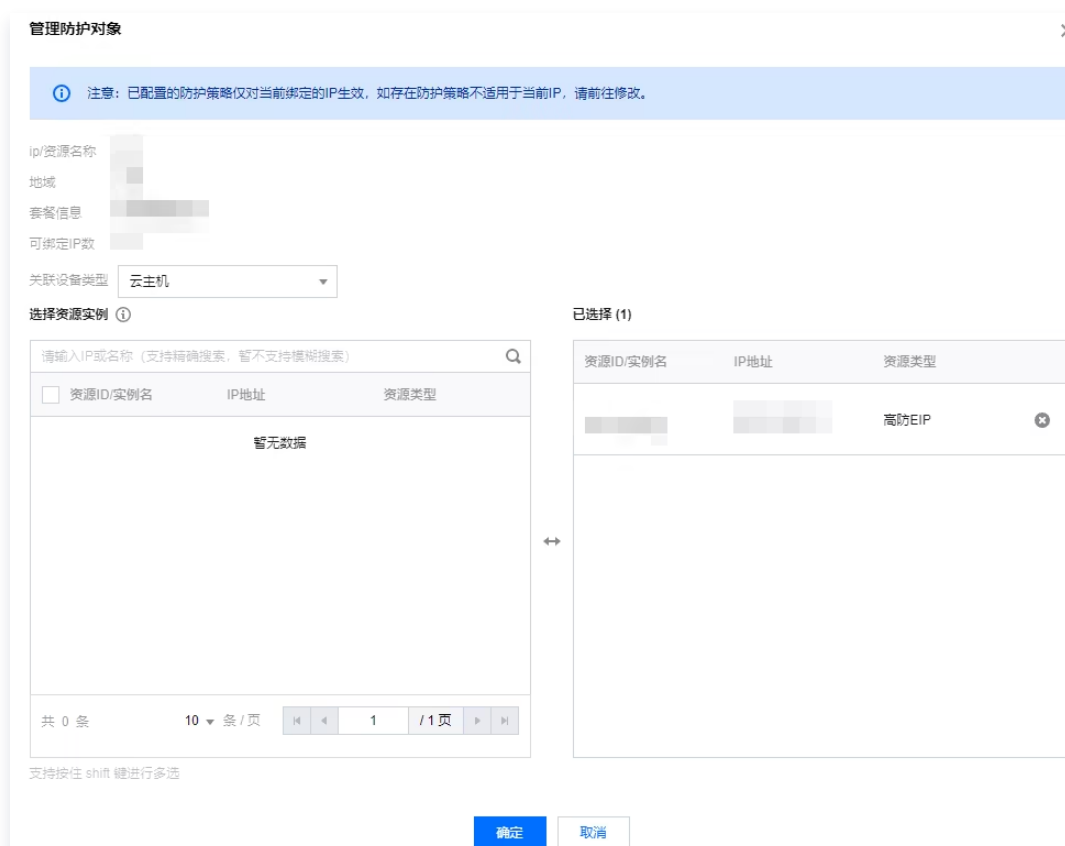
配置 DDoS 高防包

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：支持云服务器、公网负载均衡、弹性公网 IP、Web 应用防火墙等具有公网 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：2023-07-21 09:44:31

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。

① 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。

① 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：2023-07-21 09:44:31

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：2024-04-18 15:48:53

① 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，请参见 [弹性公网 IP-账户类型说明](#)。

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。

① 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 ⓘ

共享带宽包

共享带宽包

[去创建](#)

带宽上限

-

1

+

Mbps

企业版高防包

[去创建](#)

数量

-

1

+

30/40

名称 ⓘ

可选，不填默认未命名

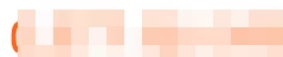
标签

▶ 增加

公网网络费用



高防EIP配置费用



IP资源费用



☐ 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，详情请参见 限额配置-使用限制
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，请参见 [弹性公网 IP-EIP 绑定云资源](#)。

平滑切换线上业务至 DDoS 高防 IP

最近更新时间：2023-07-21 09:44:31

需求背景

已上线的业务可能存在较多的特定设置和限制条件，且业务中断影响较大。因此建议用户将已上线运行的业务切换到本产品之前，参考本节相关建议，采用合适的切换方式，规避可能存在的风险。

建议

① 注意：

以下建议是基于腾讯云过往线上业务切换而总结的相关经验，用户需结合自身实际业务情况进行完善和补充，确保将切换过程中的风险降至最低。

技术维度

- 通过本地修改 hosts 文件来替代直接修改 DNS A 记录，由测试人员本地进行业务测试，验证可用性，测试延时等相关指标。
- 若已使用智能域名解析产品，可基于部分运营商或部分地域进行 DNS A 记录修改，先小范围将流量牵引到高防 IP 灰度上线再逐步完成全部业务切换。
- 减小 DNS 的 TTL，一旦出现问题可尽快切回。
- 提前准备回退方案，一旦出现问题可根据回退方案有序操作。

业务维度

- 选取备份业务、非重要业务、非关键业务先进行迁移。
- 选择业务较少的时段进行迁移。

获取客户端真实 IP（端口接入）

最近更新时间：2025-08-07 17:59:42

本文将介绍如何通过 TOA 模块获取客户端 IP，以代替 DDoS API 文档中错误的域名接入方式和缺少其他发行版编译环境依赖包安装命令的端口接入方式。

TOA 模块是一款高性能、轻量级的 TCP 连接信息采集工具，它可以在应用层获取客户端真实 IP，并将其转发给后端服务器。本文将分别介绍域名接入和端口接入两种方式下如何使用 TOA 模块获取客户端 IP。

域名接入方式

在 Nginx 反向代理的相应 location 位置配置如下内容，获取客户端 IP 的信息：

```
log_format real_ip '$http_x_forwarded_for - $remote_user [$time_local] '
    '"$request" $status $body_bytes_sent '
    '"$http_referer" "$http_user_agent"';

server {
    listen 80;
    server_name yourdomain.com;

    location / {
        proxy_pass http://backend_server;
        proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;
        access_log /var/log/nginx/access.log real_ip;
    }
}
```

其中 `proxy_set_header` 配置项用于设置 HTTP 请求头，并将客户端真实 IP 添加到请求头中；`access_log` 配置项则用于设置 Nginx 的日志格式，从而在日志中记录客户端真实 IP。

端口接入方式

后端服务加载 TOA 模块

您可以通过以下三种方式加载 TOA 模块：

- **方法一（推荐）：**如果是 Tlinux，使用 `modprobe` 加载 TOA 模块。
- **方法二：**根据源站 Linux 版本，下载对应版本已编译好的 `toa.ko` 文件直接进行加载。
- **方法三：**如果在方法一中没有找到您当前的源站 Linux 版本，您可以通过下载 TOA 源码文件自行编译并加载。

方法一：使用 modprobe 加载 TOA 模块

下图表示使用 modprobe 加载 TOA 模块失败，可以参考 [处理方法](#) 修复。

```
[root@VM-32-81-tencentos ~]# lsmod | grep -i toa
[root@VM-32-81-tencentos ~]#
```

处理方法

1. 检查内核配置文件，是否支持 TOA，可以看到 TOA 是以模块形式编译。

```
[root@VM-32-81-tencentos ~]# zcat /proc/config.gz | grep -i toa
CONFIG_TOA=m
[root@VM-32-81-tencentos ~]#
```

2. 通过 modprobe toa 加载模块。
3. 再次检查 TOA 是否已经支持，如下图所示，则代表已经支持。

```
[root@VM-32-81-tencentos ~]# modprobe toa
[root@VM-32-81-tencentos ~]# lsmod | grep -i toa
toa                20480    0
[root@VM-32-81-tencentos ~]#
```

方法二：下载已编译的 TOA 模块并加载

1. 根据腾讯云上 Linux 的版本，下载对应的 TOA 包并解压。

- CentOS

- [CentOS-7.2-x86_64.tar.gz](#)
- [CentOS-7.3-x86_64.tar.gz](#)
- [CentOS-7.4-x86_64.tar.gz](#)
- [CentOS-7.5-x86_64.tar.gz](#)
- [CentOS-7.6-x86_64.tar.gz](#)
- [CentOS-7.7-x86_64.tar.gz](#)
- [CentOS-7.8-x86_64.tar.gz](#)
- [CentOS-7.9-x86_64.tar.gz](#)

- [CentOS-8.0-x86_64.tar.gz](#)
- [CentOS-8.2-x86_64.tar.gz](#)
- Debian
 - [Debian-11.1-x86_64.tar.gz](#)
 - [Debian-10.2-x86_64.tar.gz](#)
 - [Debian-9.0-x86_64.tar.gz](#)
- SUSE Linux
 - [openSUSE-Leap-15.3-x86_64.tar.gz](#)
- Ubuntu
 - [Ubuntu-14.04.1-LTS-x86_64.tar.gz](#)
 - [Ubuntu-16.04.1-LTS-x86_64.tar.gz](#)
 - [Ubuntu-18.04.1-LTS-x86_64.tar.gz](#)
 - [Ubuntu-20.04.1-LTS-x86_64.tar.gz](#)

2. 解压完成后，执行 `cd` 命令进入刚解压的文件夹后，任意选择一种方法执行加载 TOA 模块。

- 脚本一键执行

```
/bin/bash -c "$(curl -fsSL https://edgeone-document-file-1258344699.cos.ap-guangzhou.myqcloud.com/TOA/install_toa.sh)"
```

加载成功后显示如下：

```
[root@VM-0-14-centos toa]# /bin/bash -c "$(curl -fsSL https://eo-toa-1258348367.cos.ap-shanghai.myqcloud.com/install_toa.sh)"
toa.ko install successfully
[root@VM-0-14-centos toa]#
```

- 手工配置加载

```
# 解压tar包
tar -zxvf CentOS-7.2-x86_64.tar.gz
# 进入解压后的包目录
cd CentOS-7.2-x86_64
# 加载toa模块
insmod toa.ko
# 拷贝到内核模块目录下
cp toa.ko /lib/modules/$(uname -r)/kernel/net/netfilter/ipvs/toa.ko
# 设置系统启动时自动加载toa模块
```



```
echo "insmod /lib/modules/`uname -r`/kernel/net/netfilter/ipvs/toa.ko" >> /etc/rc.local
```

可通过下面命令确认是否已加载成功：

```
lsmod | grep toa
```

出现 TOA 时表示已加载成功，如下图所示：

```
[root@VM-0-14-centos toa]# lsmod | grep toa
toa                282624  0
[root@VM-0-14-centos toa]#
```

方法三：自行编译并加载 TOA 模块

1. 安装编译环境。

- 查看当前内核版本号，确认 kernel-devel，kernel-headers 已安装，并保证版本号与内核版本保持一致。
- 确认已安装 gcc 和 make。
- 如果以上环境依赖没有安装，可参考如下命令进行安装：
 - CentOS

```
yum install -y gcc
yum install -y make
yum install -y kernel-headers kernel-devel
```

- Ubuntu/Debian

```
apt-get install -y gcc
apt-get install -y make
apt-get install -y linux-headers-$(uname -r)
```

2. 安装编译环境后，可以选择任意一种方法执行命令来完成源码的下载、编译和加载。

- 脚本一键编译并加载

```
/bin/bash -c "$(curl -fsSL https://edgeone-document-file-1258344699.cos.ap-
```

```
guangzhou.myqcloud.com/TOA/compile_install_toa.sh) "
```

○ 手工编译并加载

```
# 创建并进入编译目录
mkdir toa_compile && cd toa_compile
# 下载源代码tar包
curl -o toa.tar.gz https://edgeone-document-file-1258344699.cos.ap-guangzhou.myqcloud.com/TOA/toa.tar.gz
# 解压tar包
tar -zxvf toa.tar.gz
# 编译toa.ko文件，编译成功后会在当前目录下生成toa.ko文件
make
# 加载toa模块
insmod toa.ko
# 拷贝到内核模块目录下
cp toa.ko /lib/modules/`uname -r`/kernel/net/netfilter/ipvs/toa.ko
# 设置系统启动时自动加载toa模块
echo "insmod /lib/modules/`uname -r`/kernel/net/netfilter/ipvs/toa.ko" >> /etc/rc.local
```

3. 执行下面指令确认是否已加载成功：

```
lsmod | grep toa
```

出现 toa 则表示已加载成功，如下图所示：

```
[root@VM-32-81-tencentos ~]# lsmod | grep -i toa
toa                20480    0
```

验证获取客户端 IP 信息

如果您当前的业务是以下两种场景，只需要获取 IPv4 或 IPv6 其中一种类型客户端地址，可以按照如下步骤完成服务端加载 TOA 模块即可获取到客户端真实 IP 地址。

- 源站是 IPv4，只需要获取 IPv4 客户端地址。
- 源站是 IPv6，只需要获取 IPv6 客户端地址。

您可以通过搭建 TCP 服务，并通过另外一台服务器模拟客户端请求进行验证。

1. 在当前服务器上，可以通过 Python 创建一个 HTTP 服务来模拟 TCP 服务，如下所示：

```
# 基于python2
python2 -m SimpleHTTPServer 10000

# 基于python3
python3 -m http.server 10000
```

2. 用另一台服务器充当客户端，构造客户端请求，以 Curl 请求来模拟 TCP 请求：

```
# 利用curl发起http请求，其中域名为四层代理域名，10000为四层代理转发端口
curl -i "http://a8b7f59fc8d7e6c9.example.com.edgeonedy1.com:10000/"
```

C 语言示例代码

修改源站业务代码，同时获取 IPv4/IPv6客户端真实 IP

如果您需要同时获取到 IPv4 和 IPv6 两种类型客户端地址，则需要在加载 TOA 模块的同时修改源站业务代码。源站在建立服务监听时，可参考采用如下两种方式：

- 采用 IPv4 的地址结构 `struct sockaddr_in` 搭建服务，其监听的是 IPv4 格式的地址。

```
#include <sys/socket.h>
#include <stdio.h>
#include <unistd.h>
#include <netinet/in.h>
#include <memory.h>
#include <arpa/inet.h>

int main(int argc, char **argv){
    int l_sockfd;
    // 服务器地址采用v4结构
    struct sockaddr_in serveraddr;
    // 业务修改点：客户端地址必须采用v6结构
    struct sockaddr_in6 clientAddr;
    int server_port = 10000;

    memset(&serveraddr, 0, sizeof(serveraddr));
```

```
// 创建socket
l_sockfd = socket(AF_INET, SOCK_STREAM, 0);
if (l_sockfd == -1){
    printf("Failed to create socket.\n");
    return -1;
}

// 初始化服务器地址信息
memset(&serveraddr, 0, sizeof(struct sockaddr_in));
serveraddr.sin_family = AF_INET;
serveraddr.sin_port = htons(server_port);
serveraddr.sin_addr.s_addr = htonl(INADDR_ANY);

int isReuse = 1;
setsockopt(l_sockfd, SOL_SOCKET, SO_REUSEADDR, (const
char*)&isReuse, sizeof(isReuse));

// 关联socket和服务器地址信息
int nRet = bind(l_sockfd, (struct sockaddr*)&serveraddr,
sizeof(serveraddr));
if(-1 == nRet)
{
    printf("bind error\n");
    return -1;
}
// 监听socket
listen(l_sockfd, 5);

int clientAddrLen = sizeof(clientAddr);
memset(&clientAddr, 0, sizeof(clientAddr));
// 接受来自客户端的连接
int linkFd = accept(l_sockfd, (struct sockaddr*)&clientAddr,
&clientAddrLen);
if(-1 == linkFd)
{
    printf("accept error\n");
    return -1;
}
```

```
// 业务修改点：根据客户端sin6_family的类型，判断客户端是v4地址还是v6地址
// 当为AF_INET时，表示客户端是IPv4，将客户端地址指针转换为
struct sockaddr_in*进行获取
// 当为AF_INET6时，表示客户端是IPv6，使用struct sockaddr_in6*进行获取

if (clientAddr.sin6_family == AF_INET) {
    printf("AF_INET accept getpeername %s : %d successful\n",
        inet_ntoa(((struct sockaddr_in*)&clientAddr)-
>sin_addr),
        ntohs(((struct sockaddr_in*)&clientAddr)->sin_port));
} else if (clientAddr.sin6_family == AF_INET6) {
    char addr_p[128] = {0};
    inet_ntop(AF_INET6, (void *)&((struct
sockaddr_in6*)&clientAddr)->sin6_addr, addr_p, (socklen_t
)sizeof(addr_p));
    printf("AF_INET6 accept getpeername %s : %d successful\n",
        addr_p,
        ntohs(((struct sockaddr_in6*)&clientAddr)-
>sin6_port));
} else {
    printf("unknow sin_family:%d \n", clientAddr.sin6_family);
}
close(l_sockfd);
return 0;
}
```

- 采用 IPv6 的地址结构 `struct sockaddr_in6` 搭建服务，其监听的是 IPv6 格式的地址。

```
#include <sys/socket.h>
#include <stdio.h>
#include <unistd.h>
#include <netinet/in.h>
#include <memory.h>
#include <arpa/inet.h>

int main(int argc, char **argv)
{
```

```
int    l_sockfd;
// 服务器地址采用v6结构
struct sockaddr_in6 serveraddr;
// 客户端地址采用v6结构
struct sockaddr_in6 clientAddr;
int server_port = 10000;

memset(&serveraddr, 0, sizeof(serveraddr));

// 创建socket
l_sockfd = socket(AF_INET6, SOCK_STREAM, 0);
if (l_sockfd == -1){
    printf("Failed to create socket.\n");
    return -1;
}
// 设置服务器地址信息
memset(&serveraddr, 0, sizeof(struct sockaddr_in6));
serveraddr.sin6_family = AF_INET6;
serveraddr.sin6_port = htons(server_port);
serveraddr.sin6_addr = in6addr_any;

int isReuse = 1;
setsockopt(l_sockfd, SOL_SOCKET, SO_REUSEADDR, (const
char*)&isReuse, sizeof(isReuse));
// 关联socket和服务器地址信息
int nRet = bind(l_sockfd, (struct sockaddr*)&serveraddr,
sizeof(serveraddr));
if(-1 == nRet)
{
    printf("bind error\n");
    return -1;
}
// 监听socket
listen(l_sockfd, 5);

int clientAddrLen = sizeof(clientAddr);
memset(&clientAddr, 0, sizeof(clientAddr));
```

```
// 接受来自客户端的连接请求
int linkFd = accept(l_sockfd, (struct sockaddr*)&clientAddr,
&clientAddrLen);
if(-1 == linkFd)
{
    printf("accept error\n");
    return -1;
}

// 这里收到的客户端地址信息全部都采用v6的结构进行存储
// 其中, 客户端的IPv4地址也被映射成了一个IPv6的地址, 例
如: ::ffff:119.29.1.1
char addr_p[128] = {0};
inet_ntop(AF_INET6, (void *)&clientAddr.sin6_addr, addr_p,
(socklen_t )sizeof(addr_p));
printf("accept %s : %d successful\n", addr_p,
ntohs(clientAddr.sin6_port));

// 业务修改点: 通过系统宏定义IN6_IS_ADDR_V4MAPPED来判断一个IPv6地址是否是
IPv4的映射地址 (代表客户端是IPv4)
if(IN6_IS_ADDR_V4MAPPED(&clientAddr.sin6_addr)) {
    struct sockaddr_in real_v4_sin;
    memset (&real_v4_sin, 0, sizeof (struct sockaddr_in));
    real_v4_sin.sin_family = AF_INET;
    real_v4_sin.sin_port = clientAddr.sin6_port;
    // 读取最后四个字节即为客户端真实IPv4地址
    memcpy (&real_v4_sin.sin_addr, ((char *)&clientAddr.sin6_addr)
+ 12, 4);
    printf("connect %s successful\n",
inet_ntoa(real_v4_sin.sin_addr));
}

close(l_sockfd);
return 0;
}
```

Java 代码示例

源站在建立服务监听时，可参考采用如下两种方式：

1. 采用 IPv4 的地址结构搭建服务，IPv4、IPv6 格式的地址均可监听。
2. 采用 IPv6 的地址结构搭建服务，IPv4、IPv6 格式的地址均可监听。

采用 IPv4 的地址结构搭建服务

需要注意的是：示例代码采用 IPv4 的地址结构搭建服务，若需要采用 IPv6 的地址结构搭建服务，则需要将示例代码中的 `serverSocket.bind(new InetSocketAddress(InetAddress.getByName(IPV4_HOST), serverPort));` 更改为 `serverSocket.bind(new InetSocketAddress(InetAddress.getByName(IPV6_HOST), serverPort));`

```
import java.io.IOException;
import java.io.InputStream;
import java.io.OutputStream;
import java.net.InetAddress;
import java.net.InetSocketAddress;
import java.net.ServerSocket;
import java.net.Socket;
import java.net.SocketAddress;

public class ServerDemo {

    /** 若采用 IPv4 的地址结构搭建服务，使用 IPV4_HOST */
    public static final String IPV4_HOST = "0.0.0.0";

    /** 若采用 IPv6 的地址结构搭建服务，使用 IPV6_HOST */
    public static final String IPV6_HOST = "::";

    public static void main(String[] args) {
        int serverPort = 10000;
        try (ServerSocket serverSocket = new ServerSocket()) {
            // 设置地址复用
            serverSocket.setReuseAddress(true);
            // 绑定服务器地址和端口，这里使用 IPv4
            serverSocket.bind(new
InetSocketAddress(InetAddress.getByName(IPV4_HOST), serverPort));
            System.out.println("Server is listening on port " +
serverPort);

            while (true) {
```



```
// 接受客户端连接
Socket clientSocket = serverSocket.accept();
System.out.println("New client connected: " +
clientSocket.getRemoteSocketAddress());

// 处理客户端请求
handleClientRequest(clientSocket);
}
} catch (IOException e) {
    System.err.println("Failed to create server socket: " +
e.getMessage());
}
}

/**
 * 处理函数，具体业务具体实现，这里只做为示例
 * 此函数的作用是将 client 的输入原封不动的返回给 client
 */
private static void handleClientRequest(Socket clientSocket) {
    try (InputStream inputStream = clientSocket.getInputStream();
        OutputStream outputStream = clientSocket.getOutputStream())
    {

        // 读取客户端发来的数据
        byte[] buffer = new byte[1024];
        int bytesRead;
        while ((bytesRead = inputStream.read(buffer)) != -1) {
            // 将接收到的数据原样回复给客户端
            outputStream.write(buffer, 0, bytesRead);
        }

    } catch (IOException e) {
        // 当客户端断开连接后
        System.err.println("Failed to handle client request: " +
e.getMessage());
    } finally {
        try {
            clientSocket.close();
        } catch (IOException e) {
```

```
        System.err.println("Failed to close client socket: " +
e.getMessage());
    }
}
}
```

采用 IPv6 的地址结构搭建服务

```
import java.io.IOException;
import java.io.InputStream;
import java.io.OutputStream;
import java.net.InetAddress;
import java.net.InetSocketAddress;
import java.net.ServerSocket;
import java.net.Socket;
import java.net.SocketAddress;

public class ServerDemo {

    /** 若采用 IPv4 的地址结构搭建服务, 使用 IPV4_HOST */
    public static final String IPV4_HOST = "0.0.0.0";

    /** 若采用 IPv6 的地址结构搭建服务, 使用 IPV6_HOST */
    public static final String IPV6_HOST = "::";

    public static void main(String[] args) {
        int serverPort = 10000;
        try (ServerSocket serverSocket = new ServerSocket()) {
            // 设置地址复用
            serverSocket.setReuseAddress(true);
            // 绑定服务器地址和端口, 这里使用 IPv4
            serverSocket.bind(new
InetSocketAddress(InetAddress.getByName(IPV6_HOST), serverPort));
            System.out.println("Server is listening on port " +
serverPort);

            while (true) {
                // 接受客户端连接
```

```
        Socket clientSocket = serverSocket.accept();
        System.out.println("New client connected: " +
clientSocket.getRemoteSocketAddress());

        // 处理客户端请求
        handleClientRequest(clientSocket);
    }
} catch (IOException e) {
    System.err.println("Failed to create server socket: " +
e.getMessage());
}
}

/**
 * 处理函数，具体业务具体实现，这里只做为示例
 * 此函数的作用是将 client 的输入原封不动的返回给 client
 */
private static void handleClientRequest(Socket clientSocket) {
    try (InputStream inputStream = clientSocket.getInputStream();
        OutputStream outputStream = clientSocket.getOutputStream())
    {

        // 读取客户端发来的数据
        byte[] buffer = new byte[1024];
        int bytesRead;
        while ((bytesRead = inputStream.read(buffer)) != -1) {
            // 将接收到的数据原样回复给客户端
            outputStream.write(buffer, 0, bytesRead);
        }

    } catch (IOException e) {
        // 当客户端断开连接后
        System.err.println("Failed to handle client request: " +
e.getMessage());
    } finally {
        try {
            clientSocket.close();
        } catch (IOException e) {
            System.err.println("Failed to close client socket: " +
e.getMessage());
        }
    }
}
```

```
        }  
    }  
}
```

控制台输出结果

```
Server is listening on port 10000  
New client connected: /127.0.0.1:50680  
New client connected: /0:0:0:0:0:0:0:1:51124  
New client connected: /127.0.0.1:51136
```

更多参考

监控 TOA 运行状态

为保障 TOA 内核模块运行的稳定性，TOA 内核模块还提供了监控功能。在插入 toa.ko 内核模块后，可以通过执行以下命令方式监控 TOA 模块的工作状态。

```
cat /proc/net/toa_stats
```

TOA 运行状态如下：

```
[root@VM-32-81-tencentos ~]# cat /proc/net/toa_stats
```

		CPU0	CPU1
syn_recv_sock_toa	:	0	0
syn_recv_sock_no_toa	:	1804	1815
getname_toa_ok	:	0	0
getname_toa_mismatch	:	0	0
getname_toa_bypass	:	0	0
getname_toa_empty	:	22810	22671
vtoa_get	:	0	0
vtoa_attr_err	:	0	0
vtoa_lookup_err	:	0	0
vtoa_netlink_err	:	0	0
getname_vtoa_ipv4_err	:	0	0
getname_vtoa_ipv6_err	:	0	0

其中主要的监控指标对应的含义如下所示：

指标名称	说明
syn_recv_sock_toa	接收带有 TOA 信息的连接个数。
syn_recv_sock_no_toa	接收并不带有 TOA 信息的连接个数。
getname_toa_ok	调用 getsockopt 获取源 IP 成功即会增加此计数，另外调用 accept 函数接收客户端请求时也会增加此计数。
getname_toa_mismatch	调用 getsockopt 获取源 IP 时，当类型不匹配时，此计数增加。例如某条客户端连接内存放的是 IPv4 源 IP，并非为 IPv6 地址时，此计数便会增加。
getname_toa_empty	对某一个不含有 TOA 的客户端文件描述符调用 getsockopt 函数时，此计数便会增加。
ip6_address_alloc	当 TOA 内核模块获取 TCP 数据包中保存的源 IP、源 Port 时，会申请空间保存信息。

ip6_address_free	当连接释放时，toa 内核模块会释放先前用于保存源 IP、源 port 的内存，在所有连接都关闭的情况下，所有 CPU 的此计数相加应等于 ip6_address_alloc 的计数。
------------------	--

获取客户端真实 IP（域名接入）

最近更新时间：2025-08-08 14:31:52

本文档将为您介绍通过 DDoS 高防直接获取真实 IP 的方法，以及针对 Tomcat、Apache、Nginx 和 IIS 服务器，介绍相应的 X-Forwarded-For 配置方案及获取真实 IP 的方法。

背景信息

通常情况下，当用户进行网站访问时，浏览器可能不是直达服务器，中间会部署 CDN 及 DDoS 高防等防护服务。例如，采用这样的架构：“用户 > CDN/DDoS 高防 > 源站服务器”。

如果您已经使用 DDoS 高防服务，可直接通过高防服务获取访问者的真实 IP，您也可以通过配置网站服务器来获取访问者的真实 IP。DDoS 高防 IP 使用网站业务转发规则时，可利用 HTTP 头部的 X-Forwarded-For 字段获取客户端真实 IP。

X-Forwarded-For：是一个 HTTP 头部扩展字段，目的是使服务器可以识别通过代理等方式连接的客户端真正的 IP。

格式为：X-Forwarded-For: Client, proxy1, proxy2, proxy3……

当高防 IP 将用户的访问请求转到后端服务器时，会把请求用户的真实 IP 记录在 X-Forwarded-For 字段的首位。因此，源站应用只需要获取 HTTP 头部的 X-Forwarded-For 字段的内容即可。

通过 HTTP Header 获取真实 IP

DDoS 高防服务默认提供获取客户端真实 IP 的功能，下面推荐两种方式获取客户的来源 IP，您可以根据需要，选择任意一种方式进行使用：

方式一

DDoS 高防服务使用 X-Forwarded-For 的方式获取客户端的真实 IP 地址。

- 真实的客户端 IP 会被 DDoS 高防服务放在 HTTP 头部的 X-Forwarded-For 字段，格式如下：

```
X-Forwarded-For: 用户真实IP, 代理服务器1-IP, 代理服务器2-IP, ...
```

① 说明：

当使用此方式获取客户端真实 IP 时，获取的第一个地址即为客户端真实 IP。

- 各语言通过调用 SDK 接口获取 X-Forwarded-For 字段的方式如下：

- ASP：

```
Request.ServerVariables("HTTP_X_FORWARDED_FOR")
```

- ASP.NET(C#):

```
Request.ServerVariables["HTTP_X_FORWARDED_FOR"]
```

- PHP:

```
$_SERVER["HTTP_X_FORWARDED_FOR"]
```

- JSP:

```
request.getHeader("HTTP_X_FORWARDED_FOR")
```

方式二

DDoS 高防服务支持使用 X-Real-IP 变量，获取客户的来源 IP（使用过程中考虑了后面所经过的多层反向代理对该变量的修改）。

各种语言通过调用 SDK 接口获取 X-Real-IP 字段的方式如下：

- ASP:

```
Request.ServerVariables("HTTP_X_REAL_IP")
```

- ASP.NET(C#):

```
Request.ServerVariables["HTTP_X_REAL_IP"]
```

- PHP:

```
$_SERVER["HTTP_X_REAL_IP"]
```

- JSP:

```
request.getHeader("HTTP_X_REAL_IP")
```

访问日志打印真实 IP

Tomcat 如何在访问日志中获取真实客户端的 IP 地址

如果您的源站部署了 Tomcat 服务器，可通过启用 Tomcat 的 X-Forwarded-For 功能，获取访问者的真实 IP 地址。

1. 打开 server.xml 文件（“tomcat/conf/server.xml”），AccessLogValve 日志记录功能部分内容如下：

```
<Host name="localhost" appBase="webapps" unpackWARs="true"
autoDeploy="true">
    <Valve className="org.apache.catalina.valves.AccessLogValve"
directory="logs"
    prefix="localhost_access_log." suffix=".txt"
    pattern="%h %l %u %t \"%r\" %s %b" />
```

2. 在 pattern 中增加 “%{X-Forwarded-For}i”，修改后的 server.xml 为：

```
<Host name="localhost" appBase="webapps" unpackWARs="true"
autoDeploy="true">
    <Valve className="org.apache.catalina.valves.AccessLogValve"
directory="logs"
    prefix="localhost_access_log." suffix=".txt"
    pattern="%{X-Forwarded-For}i %h %l %u %t \"%r\" %s %b" />
</Host>
```

3. 查看 localhost_access_log 日志文件，可获取 X-Forwarded-For 对应的访问者真实 IP。

Apache 如何在访问日志中获取真实客户端的 IP 地址

如果您的源站部署了 Apache 服务器，可通过运行命令安装 Apache 的第三方模块 mod_remoteip，并修改 httpd.conf 文件获取客户 IP 地址。

1. 打开 httpd.conf 配置文件，并将文件内容修改为如下内容：
Apache 映射 xff 到 remote_addr，详情请参见 [安装 mod_remoteip](#)。
2. 定义日志格式。

```
LogFormat "%{X-Forwarded-For}i %l %u %t \"%r\" %>s %b \"%{Referer}i\"
\"%{User-Agent}i\"" common
```

3. 重启 Apache，使配置生效。

```
/[apached目录]/httpd/bin/apachectl restart
```

4. 查看 access.log 日志文件，可获取 X-Forwarded-For 对应的访问者真实 IP。

Nginx 如何在访问日志中获取真实客户端的 IP 地址

如果您的源站部署了 Nginx 反向代理，可通过在 Nginx 反向代理配置 Location 信息，后端 Web 服务器即可通过类似函数获取客户的真实 IP 地址。

1. 根据源站 Nginx 反向代理的配置，在 Nginx 反向代理的相应 location 位置配置如下内容，获取客户 IP 的信息。

```
log_format main '$remote_addr [$http_x_forwarded_for] - $remote_user  
[$time_local] ';  
  
'$request' $status $body_bytes_sent '  
'$http_referer' '$http_user_agent'";
```

2. 重启 Nginx。

通过插件映射客户端真实 IP

Tomcat 配置方案

Tomcat 配置 xff 映射到 remote_addr，详情请参见 [Tomcat 配置文档](#)。

配置示例如下：

```
<Valve className="org.apache.catalina.valves.RemoteIpValve"  
remoteIpHeader="x-forwarded-for"  
proxiesHeader="x-forwarded-by"  
internalProxies="192\.\168\.\0\.\10|192\.\168\.\0\.\11"  
trustedProxies="62\.\234\.\227\.\d{1,3}|212\.\64\.\62\.\d{1,3}"  
>
```

Apache 配置方案

Apache 映射 xff 到 remote_addr，需 [安装 mod_remoteip](#) 进行操作。

配置示例如下：

```
RemoteIPHeader X-Forwarded-For  
RemoteIPTrustedProxyList x.x.x.x/24
```

IIS 6 配置方案

如果您的源站部署了 IIS 6 服务器，您可以通过安装 F5XForwardedFor.dll 插件，从 IIS 6 服务器记录的访问日志中获取访问者真实的 IP 地址。

1. 下载并安装 [F5XForwardedFor](#) 模块。
2. 根据您的服务器的操作系统版本将 x86\Release 或者 x64\Release 目录中的 F5XForwardedFor.dll 文件拷贝至指定目录（如 C:\ISAPIFilters），同时确保 IIS 进程对该目录有读取权限。
3. 打开 IIS 管理器，找到当前开启的网站，在该网站上右键单击**属性**，打开“属性”页面。
4. 在“属性”页面，切换至 ISAPI 筛选器，单击**添加**，在弹出的窗口中，配置如下信息：
 - **筛选器名称**：F5XForwardedFor。
 - **可执行文件**：F5XForwardedFor.dll 的完整路径，例如：C:\ISAPIFilters\F5XForwardedFor.dll。
5. 单击**确定**，重启 IIS 6 服务器。
6. 查看 IIS 6 服务器记录的访问日志（默认的日志路径为：C:\WINDOWS\system32\LogFiles\，IIS 日志的文件名称以 .log 为后缀），可获取 X-Forwarded-For 对应的访问者真实 IP。

IIS 7 配置方案

如果您的源站部署了 IIS 7 服务器，您可以通过安装 F5XForwardedFor 模块，从 IIS 7 服务器记录的访问日志中，获取访问者真实的 IP 地址。

1. 下载并安装 [F5XForwardedFor](#) 模块。
2. 根据服务器的操作系统版本将 x86\Release（或 x64\Release）目录中的 F5XFFHttpModule.dll 和 F5XFFHttpModule.ini 文件拷贝到指定目录（如 C:\x_forwarded_for\x86 或 C:\x_forwarded_for\x64），并确保 IIS 进程对该目录有读取权限。
3. 在 IIS 服务器的选择项中，双击**模块**，进入“模块”界面。
4. 单击**配置本机模块**，在弹出的对话框中，单击**注册**，按操作系统选择注册模块注册已下载的 DLL 文件。
 - x86 操作系统：注册模块 x_forwarded_for_x86
 - 名称：x_forwarded_for_x86
 - 路径：C:\x_forwarded_for\x86\F5XFFHttpModule.dll
 - x64 操作系统：注册模块 x_forwarded_for_x64
 - 名称：x_forwarded_for_x64
 - 路径：C:\x_forwarded_for\x64\F5XFFHttpModule.dll
5. 注册完成后，勾选新注册的模块（x_forwarded_for_x86 或 x_forwarded_for_x64）并单击**确定**。
6. 在 ISAPI 和 CGI 限制中，按操作系统添加已注册的 DLL 文件，并将其“限制”改为“允许”。
 - x86 操作系统：
 - ISAPI 或 CGI 路径：C:\x_forwarded_for\x86\F5XFFHttpModule.dll
 - 描述：x86
 - x64 操作系统：

- ISAPI 或 CGI 路径: “C:\x_forwarded_for\x64\F5XFFHttpModule.dll”
- 描述: x64

7. 重启 IIS 7 服务器, 等待配置生效。

8. 查看 IIS 7 服务器记录的访问日志 (默认的日志路径为: C:\WINDOWS\system32\LogFiles\ , IIS 日志的文件名称以 .log 为后缀), 可获取 X-Forwarded-For 对应的访问者真实 IP。

与源站结合的防护调度方案

最近更新时间：2024-04-18 15:48:53

需求背景

部分用户的业务对延时要求严格，或者受限于业务要求常态化情况下必须直接访问源站，此时可考虑结合源站的防护调度方案。

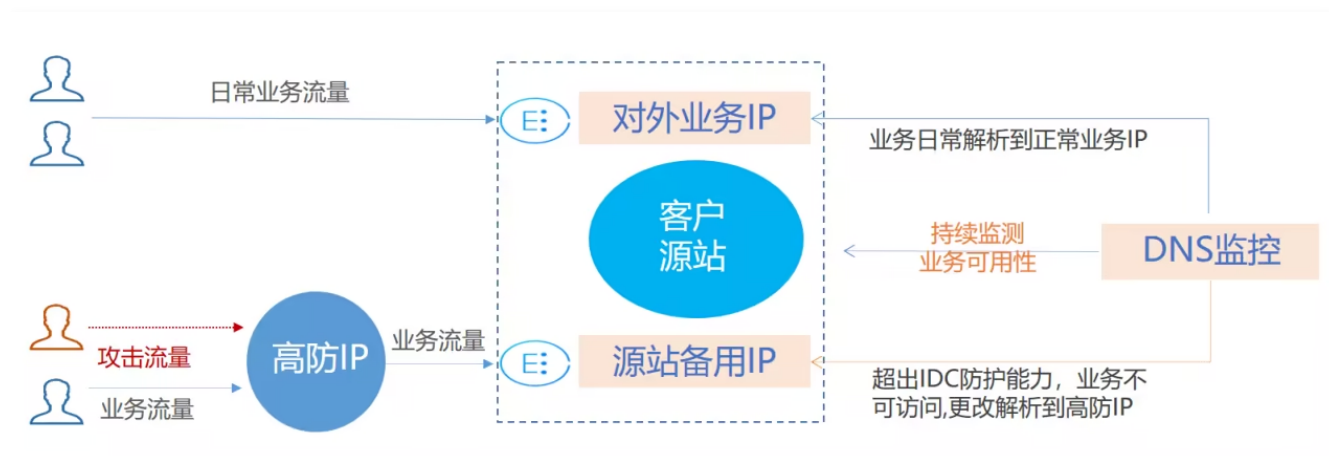
该方案可满足流量常态化情况下直接访问源站，但遭到攻击后可迅速具备防护能力的要求。

防护方案

与源站结合的防护调度方案如下图：

说明：

本方案依赖于 DNS 服务商，需要具备监控和智能切换功能。



方案说明

本方案主要由高防 IP、DNS 监控、客户源站的对外业务 IP 和源站备用 IP 组成。

- 常态化情况下，业务的域名解析到正常的对外业务 IP，业务流量直接访问源站。DNS 监控实时监控源站业务是否可以正常访问。
- 当 DNS 监控检测到正常的对外业务 IP 无法访问时，依据智能切换的设置规则，迅速将业务域名解析到高防 IP 上。高防 IP 对攻击流量进行清洗，将干净的业务流量转发到源站的备用 IP，从而保障业务可用。

注意：

为避免由于网络抖动等因素造成的误切换，确保监控效果，建议进行手动切换。

方案效果

- 满足常态化情况下直接访问源站的需求。

- 适用于对延时要求非常严格的业务。
- 遭到攻击超出源站防护能力后，可自动切换到高防 IP 进行防护。

建议与注意事项

- 需提前完成源站备用 IP、高防 IP 转发规则等配置。
- 建议将源站备用 IP 与正常的业务 IP 分布在不同的物理线路，以获得更好的防护效果。
- 建议定期进行验证和演练，熟悉方案细节，解决可能存在的问题。

CC 防护策略配置流程及注意事项

最近更新时间：2025-08-08 16:07:32

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



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**。

① 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](#)。

CC防护开关及清洗阈值 ①

CC防护根据访问模式和连接状态判定恶意行为，阻断黑客的攻击。宽松模式仅拦截明确的攻击请求，适中模式拦截显著的攻击请求，严格模式会拦截所有疑似攻击请求。如果严格模式无法拦截正在遭受的攻击或宽松模式无法避免误拦截业务，请联系技术支持。[了解详情](#)

CC防护  关闭总开关后，以下防护策略均失效，不会拦截CC攻击行为

清洗阈值 自定义 123 QPS

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](#)。

- ① 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。

新建精准防护

关联高防IP

bgr

原

①

协议

☒ HTTP

☐ HTTPS

域名

请选择

匹配条件

字段	逻辑	值
添加		

匹配动作

人机校验

确定

取消

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。

匹配条件

- 丢弃：不做人机识别，直接丢弃。
- 人机校验：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](#)。

① 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。

自定义规则设置

关联高防IP

bgpi



协议



HTTP



HTTPS

域名

请选择



字段

模式

值

添加

频率限制策略

人机校验

检测条件

每

秒

访问

次



惩罚时间

秒

确定

取消

字段	字段描述
Cookie	访问请求中携带的 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：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：2025-11-05 14:57:02

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**。

批量导入四层转发规则



高防IP

提示：一次最多添加50条转发规则

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（多个回源域名中间由逗号分隔）。一行只能填写一条转发规则。

确定

取消

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：2025-03-19 20:47:22

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。

① 说明：

- 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 [云解析 DNS](#)。

操作步骤

- 登录 [DDoS 防护（新版）控制台](#)，在左侧导航栏中，单击 [智能调度](#)。
- 在智能调度页面，单击 [新建调度](#)，系统自动生成一个 CNAME 记录。

新建调度							请输入cname名称	Q
名称	CNAME	解析状态 ▾	关联防护实例	调度模式	最后修改时间	操作		
示例名称	示例CNAME.m	正在运行	3 个关联资源 ①	优先级	2025-03-19 20:47:22	编辑 删除		
示例名称	示例CNAME.m	正在运行	1 个关联资源 ①	优先级	2025-03-19 20:47:22	编辑 删除		

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。

新建智能调度

名称

未命名

CNAME

z

TTL值

60 秒

模式

优先级模式

定向模式

回切时间

60

联动资源

[添加高防资源IP](#) [添加非高防资源IP](#)

IPv4

高防资源	IP协议	优先级	线路	地区	运行状态	域名解析	操作
暂无数据							

IPv6

高防资源	IP协议	优先级	线路	地区	运行状态	域名解析	操作
暂无数据							

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。

添加高防资源IP

选择资源类型

高防IP

选择资源实例

高防包

高防IP

已选择 (0)

资源ID/实例名	IP地址	资源类型
----------	------	------

资源ID/实例名	IP地址	资源类型
☐ bgpip-		高防IP
☐ bgpip-		高防IP
☐ bgpip-		高防IP
☐ bgpip-		高防IP
☐ bgpip-		高防IP
☐ bgpip-		高防IP
☐ bgpip-		高防IP
☐ bgpip-		高防IP

支持按住 shift 键进行多选

确定

取消

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。

资源ID	IP地址	线路	优先级	地区	运行状态	域名解析	操作
net-00000		联通	100	华东地区(上海)	运行中	☒	解除绑定
bgpip-00000		电信	100	华东地区(上海)	运行中	☒	解除绑定
bgp-00000		移动	100	华东地区(上海)	运行中	☒	解除绑定

云服务器被封堵后快速恢复业务

最近更新时间：2025-11-05 14:57:02

DDoS 攻击是指通过控制大量计算机或网络僵尸来同时访问目标服务器，造成目标服务器的拥堵和负载过重，从而使合法用户无法正常访问该服务器。这种攻击可以严重影响网站或服务的可用性，并给被攻击者带来巨大的损失。您可以根据业务情况，选择合适的方案进行恢复业务。

方案一：等待到期自动解封，恢复业务

如果您的网络服务遭受了 DDoS 攻击并被封堵，您可以等待系统自动解封。DDoS 基础防护默认情况下，封堵 2~24 小时后自动解封（具体封堵时长，请以实际封堵时长为准）。您可以登录 [DDoS 防护（新版）控制台](#)，在左侧导航中，选择[解封中心](#)页面，查看自助解封剩余次数。

您也可以通过 [站内信](#)、手机短信、邮箱查看预计解封时间，再结合业务交付情况，评估是否需要等待自动解封。

方案二：使用 DDoS 防护手动解封，恢复业务

如果您的业务已经接入 [DDoS 防护](#)，则可以手动解除封堵。具体操作，请参见 [自助解封](#)。

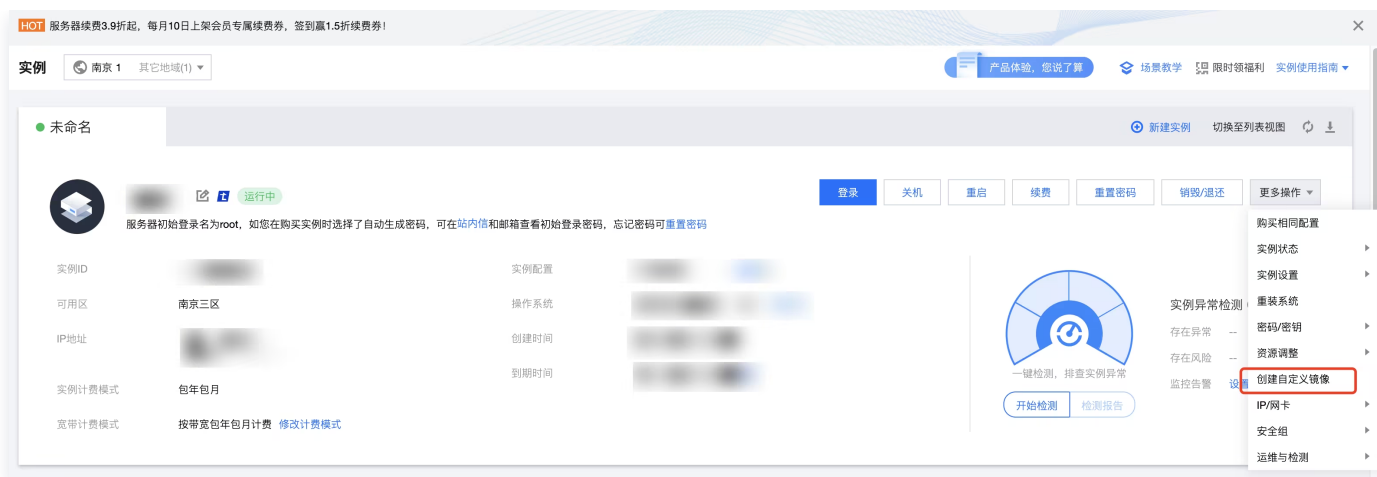
① 注意：

- 使用 DDoS 高防包（不包含轻量版、普惠版）和 DDoS 高防 IP 的用户每天将拥有三次自助解封机会，当天超过三次后将无法进行解封操作。
- 解封可能失败（解封失败不会扣减您的剩余解封次数），请您耐心等待一段时间后再次尝试。
- 在执行解封操作前，建议您先查看预计解封时间，预计解封时间可能会推后。
- 如果当天自助解封配额为0，建议提升保底防护能力或弹性防护能力，以便足够防御大流量攻击，避免被持续封堵。

通过以上步骤，您应该能够成功地手动解封并恢复业务，或者可以选择直接购买高防产品以便恢复。针对小流量攻击场景，可以选购 [DDoS 基础防护（加强版）](#)，有更高防护要求，可以选购 [DDoS 高防包](#) 或 [DDoS 高防 IP](#)。

方案三：使用镜像创建配置相同的云服务器实例，更换业务服务器

1. 选择进入封堵的云服务器，然后创建自定义镜像，具体操作，请参见 [创建自定义镜像](#)。



说明：

除了使用腾讯云提供的公共镜像、服务市场镜像外，您还可以创建自定义镜像。创建自定义镜像后，您可以在腾讯云控制台快速创建与该镜像相同配置的云服务器实例。

2. 使用步骤1中创建的自定义镜像，快速创建相同配置的云服务器实例。具体操作请参见 [通过自定义镜像创建实例](#)。

方案四：更换云服务器实例的公网 IP

1. 在 [公网 IP 控制台](#) 申请新的弹性公网 IP。具体操作，请参见 [申请 EIP](#)。

申请EIP

IP 地址类型①

☒ 常规 BGP IP

普通线路 BGP IP，用于平衡网络质量与成本

☐ 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

计费模式①

按流量

包月带宽

按小时带宽

共享带宽包

带宽上限

20

40

60

100

—

1

+

Mbps

数量

—

1

+

您当前地域下已有 0 个 EIP，还可以申请 20 个 EIP

名称①

可选，不填默认未命名

高级选项

▶ 标签

公网网络费用

1GB

IP资源费用

1小时

仅在IP闲置时收取，绑定云资源后不收取。

☐ 同意

[《腾讯云 EIP 服务协议》](#)

[《欠费规则》](#)

确定

取消

2. 解绑已绑定到云服务器实例上的弹性公网 IP。具体操作请参见 [解绑 EIP](#) 或者 [退还普通公网 IP](#)。

3. 绑定新的弹性公网 IP 至云服务器实例上。具体操作请参见 [EIP 绑定云资源](#)。

① 说明：

- 若标准账户类型的云服务器实例已存在普通公网 IP，则需先释放普通公网 IP，才能绑定 EIP。
- 若传统账户类型的云服务器实例已存在普通公网 IP，则绑定 EIP 后会释放当前云服务器实例的普通公网 IP。
- EIP 绑定云服务器实例的数量限制，根据云服务器实例 CPU 配置的差异有所不同，请参见 [使用限制](#)。

轻量应用服务器封堵后快速恢复业务

最近更新时间：2026-09-11 14:24:33

如果 [轻量应用服务器](#) 突然遭受 DDoS 攻击，轻量云服务器默认提供2Gbps的防护。但鉴于当前常见的攻击模式，一旦遭到攻击，服务器极有可能立即宕机。DDoS 防护机制如下：一旦遭受攻击，且攻击流量超过2Gbps，系统便会将主机的 IP 地址隔离，使其无法从外网访问，这类似于被置于“小黑屋”。当攻击停止后，服务器提供自助解封3次。如果服务器被攻击短暂隔离解封次数超过3次后，服务器将会进入隔离24小时的状态。

您可以根据业务情况，选择合适的方案进行恢复业务。

方案一：等待到期自动解封，恢复业务

轻量应用服务器可能会因被 DDoS 攻击被封堵隔离，被隔离的轻量应用服务器在控制台显示为“BANNING”状态。

如果您的网络服务遭受了 DDoS 攻击并被封堵，可以等待系统自动解封。DDoS 基础防护默认情况下，封堵2~24小时后自动解封（具体封堵时长，请以实际封堵时长为准）。具体可以查看下方自动解封的操作步骤。

1. 按照站内信、手机短信、邮箱查看预计解封时间，再结合业务交付情况，评估是否需要等待自动解封。
2. 可以登录 [DDoS 防护（新版）控制台](#)，在左侧导航中，选择[解封中心](#)页面，查看自助解封剩余次数。

① 说明：

如超过自助解封次数后，将不再支持自助解封。

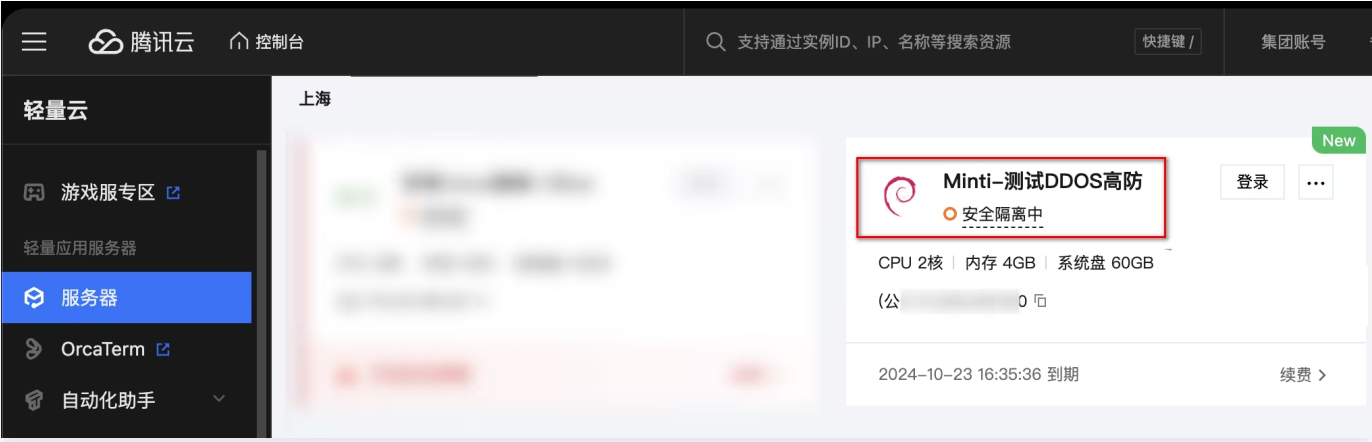
方案二：使用 DDoS 防护手动解封，恢复业务

若您的主机 IP 被禁，并希望立即解封，可使用手动解封功能。使用该功能时，您需要已成功购买 [DDoS 高防包（轻量版）](#)。

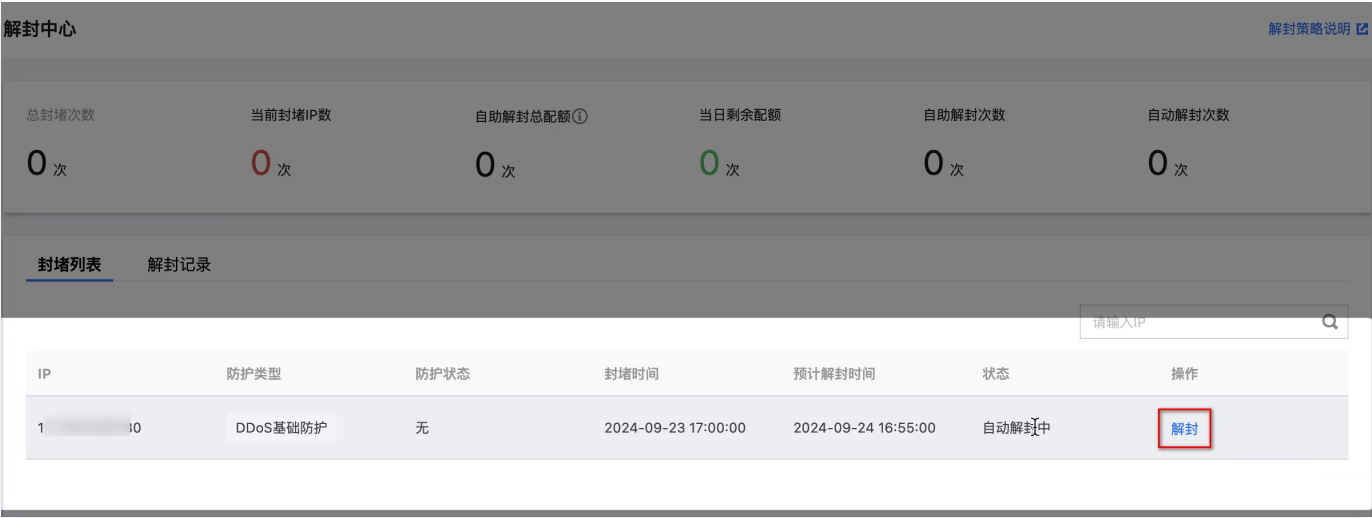
① 说明：

- DDoS 高防包（轻量版）仅适用于轻量应用服务器。
- DDoS 高防包（轻量版）产品规格为1IP+最高10Gbps防护+1年（仅此一种规格）。
- 自2023年02月27日起购买的 DDoS 高防包（轻量版），每月提供3次自助解封能力。自助解封能力仅可用于解封轻量服务器资源，具体操作请参考 [自助解封操作](#)。

1. 登录 [轻量应用服务器](#)，在左侧操作栏中，单击[服务器](#)。
2. 在服务器页面，查看安全隔离中的服务器。



3. 前往 DDoS 防护控制台的 [解封中心](#) 页面，在封堵列表中，单击目录 IP 操作列的解封。



方案三：使用镜像创建配置相同的 LH 服务器，开通新轻量

腾讯云轻量服务器遭受攻击后，尽管服务器的公网 IP 被封锁，内网依然保持有效，主机仍然可用，只是无法从互联网进行访问。在这种情况下，可以使用轻量服务器的镜像功能进行恢复，但这需要新开一台轻量服务器。
原理是：旧轻量制作镜像 A > 新轻量开通时装系统时选择镜像 A > 新轻量开通 > 域名解析到新轻量。

1. 选择被隔离的服务器，单击制作镜像，制作旧轻量制作镜像 A。具体操作步骤，请参见 [创建自定义镜像](#)。



2. 在制作自定义镜像页面，选择自定义镜像 A，输入镜像名称、镜像描述，并单击开始制作。

制作自定义镜像

自定义镜像配额及计费说明:

- 每个地域免费自定义镜像配额: 5 个, 超过5个后将会按照超出配额个数进行收费, 按小时结算。
- 每个地域自定义镜像配额: 20 个。
- 如果您的账户处于欠费状态, 将会导致制作镜像失败。

制作镜像须知:

- 开机制作镜像 仅能捕获当前已经在系统盘上的数据, 而无法将在内存中的数据记录下来。因此, 为了保证尽可能恢复完整的数据, 建议您在制作前进行 sync 操作, 下刷内存数据。
- Linux实例制作自定义镜像请确认 `/etc/fstab` 中不包含数据盘配置, 否则会导致使用该镜像创建的实例无法正常启动。如果有挂载数据盘, 需要注释或删除您在 `/etc/fstab` 中自行配置的数据盘的相关配置。
- 自定义镜像创建完成后, 您可以前往 镜像页面 进行管理, 目前轻量应用服务器支持 跨地域复制镜像, 或者 共享镜像至云服务器CVM。
- 实例开机状态下制作镜像约需30分钟或者更长时间, 与磁盘大小有关, 请耐心等待。

您已选择1台实例

实例ID/名称	套餐配置	地域	操作系统
lhi- Mi- S高防	CPU - 2 核 内存 - 2 GB 系统盘 - SSD云硬盘 40GB 流量包 - 200GB/月 (带宽: 3Mbps)	广州	Debian 12.0 64bit

镜像名称 *

请输入镜像名称

镜像描述

你还可以输入60个字符

开始制作

取消

- 完成创建自定义镜像，前往 [自定义镜像](#) 列表页面查看。
- 使用自定义镜像快速创建轻量应用服务器实例，具体步骤参考 [使用自定义镜像创建实例](#)。



故障处理

配置安全组阻止入站后，仍遭受到 DDoS 攻击

最近更新时间：2024-12-04 15:41:02

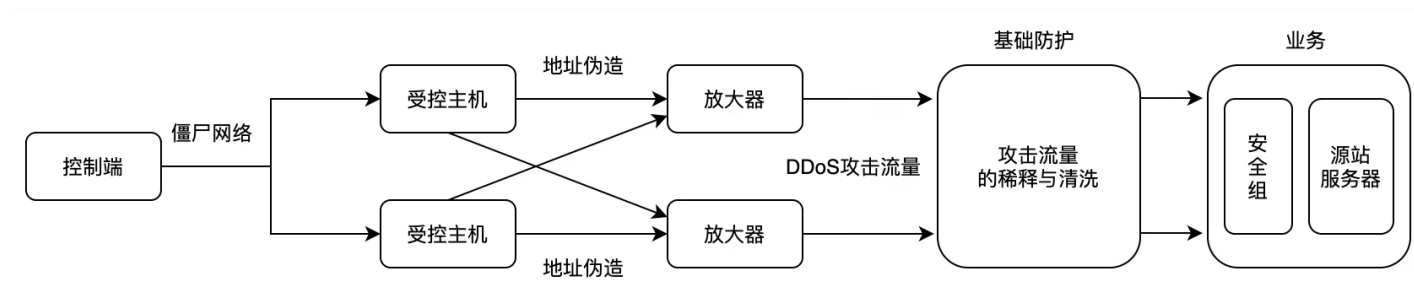
现象描述

配置了安全组规则阻止入站后，业务仍遭受到 DDoS 攻击。

可能原因

常见 DDoS 攻击方法包括：攻击网络和带宽资源、攻击系统资源、攻击应用资源等方式。

常见攻击流程如下图所示：



1. 控制端通过僵尸网络等方式控制大量主机，通过放大、反射等方式构造大量 DDoS 流量攻击服务器。
2. 云业务服务提供商会提供一定攻击流量稀释与清洗的 DDoS 基础防护。
3. 用户进行安全组的入站策略等配置，只能达到基于 IP 和端口的防护，此时经过基础防护若不能完全将攻击流量进行稀释与清洗，攻击者仍可以达到利用 DDoS 攻击流量占用网络和带宽资源等目的。

解决思路

购买 DDoS 高防包或 DDoS 高防 IP，获得更强的防护能力，抵御大流量 DDoS 攻击。

处理步骤

DDoS 高防包、DDoS 高防 IP 购买方法请参见 [购买指引](#)。

① 说明

- 防护对象：
 - DDoS 高防包只针对腾讯云内的用户提供 DDoS 防护能力。
 - DDoS 高防 IP 面向云内外用户，支持网站域名和业务端口接入防护。
- 接入：
 - DDoS 高防包的接入配置更加便捷，无需变更公网 IP 地址。

- DDoS 高防 IP 需修改 DNS 解析或修改业务 IP 后才能接入防护。

详情请参见 [DDoS 防护解决方案对比](#)。

公网 IP 遭遇 DDoS 攻击

最近更新时间：2026-09-11 14:24:32

现象描述

业务遭受 DDoS 大流量攻击，消耗目标服务器性能/网络带宽，造成服务器无法正常提供服务。

可能原因

用户 IP 遭受的攻击大小，超过了腾讯云赠送的基础防护能力。

解决思路

● 更换公网 IP（攻击停止时，临时方案）

攻击者发起 DDoS 攻击是针对具体业务 IP，通过临时更换 IP，只能临时规避被封堵的问题，无法根本解决，攻击者可能随时针对新 IP 发起第二次攻击，产生二次影响。

● 购买高防产品（推荐方案）

通过购买 DDoS 高防产品，提升 IP 的防护能力，抵御大流量攻击，如攻击流量超过了高防包所在地域的能力，可按需选择更大防护能力的高防 IP 产品。

处理步骤

更换公网 IP（攻击停止时，临时方案）

更换公网 IP 相关限制如下：

- 单个账号单个地域不超过3次/天。
- 单台实例仅允许更换1次公网 IP。
- 更换后原公网 IP 将被释放。

更换操作详情，请参见 [更换公网 IP 地址](#)。

购买配置高防产品（推荐方案）

- 购买并配置 DDoS 高防包、DDoS 高防 IP 请参见 [购买指引](#) 和 [快速入门](#)。
- DDoS 高防包和 DDoS 高防 IP 的对比，请参见 [DDoS 防护解决方案对比](#)。

业务被大流量攻击导致封堵

最近更新时间：2024-04-18 15:48:53

现象描述

业务被大流量攻击导致 IP 封堵，业务无法访问。

可能原因

- 超过防护流量阈值，导致被封堵。
- 攻击还在持续，无法进行自动解封。

解决思路

- DDoS基础防护：默认情况下，封堵2~24小时后自动解封（具体封堵时长，请以实际封堵时长为准）。
- DDoS 高防用户每天拥有三次自助解封机会，当天超过三次后将无法进行解封操作。系统将在每天零点时重置自助解封次数，当天未使用的解封次数不会累计到次日。

如解封次数用完：

- 未购买 DDoS 高防包的客户，建议用户购买高防包，首次绑定设备可进行解封。
- 已购买 DDoS 高防包的客户，建议客户升级防护套餐，可提前解除封堵。

处理步骤

1. 登录 [DDoS 防护（新版）控制台](#)，在左侧导航中，选择[解封中心](#)页面，查看自助解封剩余次数。

- 若自助解封剩余次数为0，则跳转到 [步骤5](#)，或等待自动解封。
- 若自助解封剩余次数不为0，则跳转到 [步骤2](#)。

① 说明：

自动解封时间，请参考 [DDoS 防护（新版）控制台 自助解封 > 近期安全事件](#) 页面的“预计解封时间”项。

解封中心						解封策略说明
总封堵次数	当前封堵IP数	自助解封总配额	当日剩余配额	自助解封次数	自动解封次数	
739 次	0 次	3 次	3 次	40 次	199 次	
封堵列表						
解封记录						
IP	防护类型	防护状态	封堵时间	预计解封时间	状态	操作
请输入IP						

2. 查看攻击是否已停止，请选择[防护概览](#)查看。

- 若是，则跳转到 [步骤3](#)。
- 若否，待攻击停止时，继续执行解封操作，执行 [步骤3](#)。

① 说明：

攻击如果持续进行未停止，则无法进行解封，需等待攻击结束自助解封或自动解封。

3. 在左侧导航中，选择**解封中心**，进入解封操作页面。

4. 在解封操作页面，找到状态为“自动解封中”的防护 IP，在右侧操作栏中，单击**解封**。

解封中心

解封策略说明

总封禁次数

734次

当前封禁IP数

1次

自助解封总配额

3次

当日剩余配额

3次

自助解封次数

40次

自动解封次数

195次

封禁列表

解封记录

请输入IP

IP	防护类型	防护状态	封禁时间	预计解封时间	状态	操作
	DDoS基础防护	无	2023-06-08 16:06:00	2023-06-09 17:40:00	自动解封中	解封

5. 不同 DDoS 防护产品的用户，对应建议如下：

- 如果是 DDoS 基础防护用户，建议用户购买高防包（支持防护地域：广州、上海和北京），首次绑定设备可进行解封。
- 如果是 DDoS 高防用户，建议用户升级防护套餐（增加防护次数或防护 IP 数），可提前解除封堵。

DDoS 攻击未达到阈值业务 IP 被封堵

最近更新时间：2025-06-10 09:29:22

现象描述

攻击流量没有达到购买封堵阈值，但 IP 被封堵。

可能原因

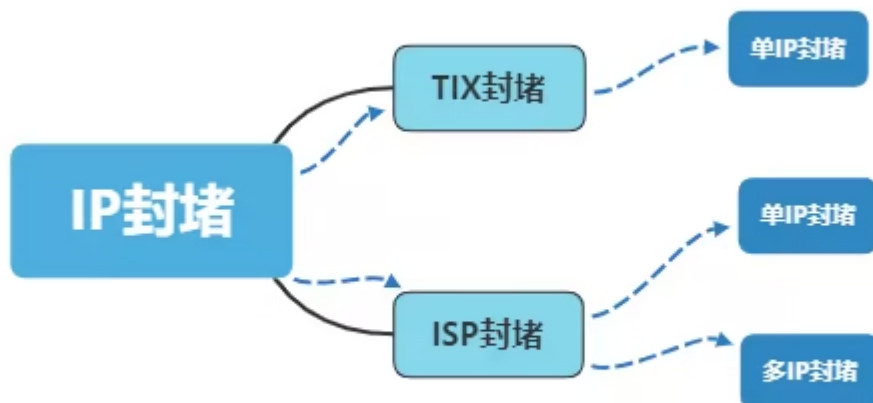
已购买 DDoS 高防包，所有出网口的攻击流量总和未达到购买阈值便进行封堵。计算方式：所有出网口的攻击流量与购买阈值对比。

1. 根据封堵的节点位置分为两种封堵。

- TIX 封堵：为腾讯的出口网关进行封堵，封堵的阈值是可控的。
- ISP 封堵：为运营商封堵，封堵的阈值基本固定的。

2. 在 ISP 封堵的情况下分为两种方式封堵。

- 单 IP 封堵：当一个 IP 的流量达到某个出口单 IP 封堵阈值（根据出口带宽设置）时封堵。
- 多 IP 封堵：当某个检测区间 IDC 的总流量（攻击流量 + 业务流量）超过多 IP 封堵阈值。



解决思路

等待攻击结束后进行自助解封或者自动解封。

处理步骤

1. 登录 [DDoS 防护管理控制台](#)，在左侧导航中，选择[解封中心](#)页面，查看自助解封剩余次数。

- 若自助解封剩余次数为0，则跳转到 [步骤5](#)，或等待自动解封。

- 若自助解封剩余次数不为0，则跳转到 [步骤2](#)。

① 说明：

自动解封时间，请参考控制台 [解封中心](#) 页面的“预计解封时间”项。

解封中心						解封策略说明
总封堵次数	当前封堵IP数	自助解封总配额	当日剩余配额	自助解封次数	自动解封次数	
739 次	0 次	3 次	3 次	40 次	199 次	
封堵列表						解封记录
IP	防护类型	防护状态	封堵时间	预计解封时间	状态	操作
请输入IP						

2. 查看攻击是否已停止，请选择 [防护概览](#) 查看。

- 若是，则跳转到 [步骤3](#)。
- 若否，待攻击停止时，继续执行解封操作，执行 [步骤3](#)。

① 说明：

攻击如果持续进行未停止，则无法进行解封，需等待攻击结束自助解封或自动解封。

3. 在左侧导航中，选择[解封中心](#)，进入解封操作页面。

4. 在解封操作页面，找到状态为“自动解封中”的防护 IP，在右侧操作栏中，单击[解封](#)。

解封中心						解封策略说明
总封堵次数	当前封堵IP数	自助解封总配额	当日剩余配额	自助解封次数	自动解封次数	
734 次	1 次	3 次	3 次	40 次	195 次	
封堵列表						解封记录
IP	防护类型	防护状态	封堵时间	预计解封时间	状态	操作
	DDoS基础防护	无	2023-06-08 16:06:00	2023-06-09 17:40:00	自动解封中	解封

5. 不同 DDoS 防护产品的用户，对应建议如下：

- 如果是 DDoS 基础防护用户，建议用户购买高防包（支持防护地域：广州、上海和北京），首次绑定设备可进行解封。
- 如果是 DDoS 高防用户，建议用户升级防护套餐（增加防护次数或防护 IP 数），可提前解除封堵。

使用高防 IP，业务访问出现502报错

最近更新时间：2025-08-07 17:59:42

现象描述

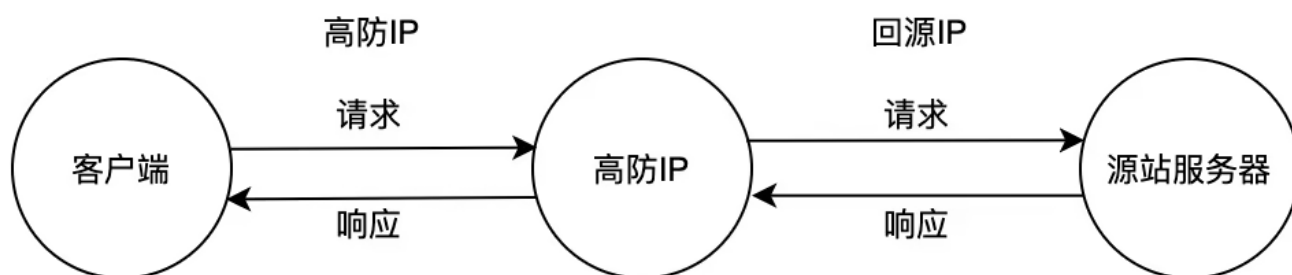
使用高防 IP 之后，访问业务出现502报错：Bad Gateway，如图所示：

502 Bad Gateway

nginx/1.18.0

可能原因

使用高防 IP 后的业务流量走向图：



原因一：回源 IP 被源站拦截或限速

在配置高防 IP 后，源站服务器的 IP 被高防 IP 在中间代理而被隐藏。所有经过高防 IP 服务访问的客户端源 IP 都会变成高防 IP 的回源 IP。源站服务器接收到的访问请求都是来自高防 IP 回源段，而高防 IP 回源段的 IP 数量有限，分摊过后每个回源 IP 访问源站服务器的请求量较大。

若源站服务器配置了 DDoS 攻击等相关安全防护策略，将有可能触发 DDoS 防护策略，导致将回源 IP 限速甚至拦截。

原因二：源站本身异常，导致响应高防的请求超时

导致异常的可能原因：

1. 在使用高防 IP 之前，源站 IP 暴露，被恶意攻击导致故障。
2. 源站服务器机房物理故障。
3. 服务器内存、CPU 占用过高，导致性能降低。
4. 源站服务器中 Apache、Nginx 等 Web 程序异常。

5. 公网转发至源站服务器间链路出现故障。

原因三：网络抖动或者链路故障

公网网络质量不佳造成的业务访问不稳定，提示502报错。

解决思路

原因一：解决思路

通过腾讯云拨测平台对源站 IP 和高防 IP 进行拨测，对比源站 IP 和高防 IP 的访问情况，拨测方式可以参考 [腾讯云拨测使用说明](#)。

如源站 IP 正常、高防 IP 大范围异常，则可以判断为高防回源 IP 被源站服务器拦截或限速导致，建议进行高防回源 IP 加白操作。

详细处理步骤请参见 [原因一：处理步骤](#)。

原因二：解决思路

通过将本地主机的解析结果修改为源站来验证源站本身是否正常，首先修改本地 hosts 文件，确认 hosts 绑定已经生效之后，使用域名进行验证源站是否可以正常访问，如不能正常访问，可以尝试做如下处理：

1. 源站 IP 保护。详情步骤请参见 [处理措施1](#)。
2. 请相关人员进行机房故障检查，修复物理故障。详情步骤请参见 [处理措施2](#)。
3. 确认 Web 服务是否正常并修复。详情步骤请参见 [处理措施3](#)。
4. 检查服务器进程占用，内存占用等性能参数是否正常并恢复至正常状态。详情步骤请参见 [处理措施4](#)。
5. 查看网络层面进行排查或者源站链路监控设备监控到的链路状态，也可通过更换链路测试进行验证与规避。详情步骤请参见 [处理措施5](#)。

详细处理步骤请参见 [原因二：处理步骤](#)。

原因三：解决思路

确定是否存在链路故障情况并联系网络服务商进行修复。

详细处理步骤请参见 [原因三：处理步骤](#)。

处理步骤

原因一：处理步骤

将高防 IP 回源段添加至防火墙、主机安全防护软件的白名单中进行放行，下面以 CentOS 6.5 操作系统的防火墙添加白名单为例：

1. 执行如下命令，查看 Linux 防火墙的状态。

```
service iptables status
```

如果控制台提示 Chain INPUT、Chain FORWARD 以及 Chain OUTPUT 项下没有任何规则条目，说明防火墙还未开启。

service iptables status

```
[root@localhost /]# service iptables status
Table: filter
Chain INPUT (policy ACCEPT)
num  target      prot opt source                destination

Chain FORWARD (policy ACCEPT)
num  target      prot opt source                destination

Chain OUTPUT (policy ACCEPT)
num  target      prot opt source                destination
```

2. 执行如下命令，查看防火墙配置文件。

```
cat /etc/sysconfig/iptables
```

根据业务需求，确保防火墙没有额外的黑白名单设置后，将防火墙开启，防止直接打开防火墙之后对业务造成影响。

3. 执行如下命令，开启防火墙。

```
service iptables start
```

service iptables start

```
[root@localhost /]# service iptables start
iptables: Applying firewall rules: [ OK ]
```

4. 执行如下命令，再次查看防火墙状态。

```
service iptables status
```


如果控制台提示 Chain INPUT、Chain FORWARD 以及 Chain OUTPUT 任意项显示规则条目，证明防火墙已经打开。

```
[root@localhost ~]# service iptables status
Table: filter
Chain INPUT (policy ACCEPT)
num target      prot opt source                destination              state
1  ACCEPT        all  --  0.0.0.0/0              0.0.0.0/0                state RELATED, ESTABLISHED
2  ACCEPT        icmp --  0.0.0.0/0              0.0.0.0/0
3  ACCEPT        all  --  0.0.0.0/0              0.0.0.0/0
4  ACCEPT        tcp  --  0.0.0.0/0              0.0.0.0/0                state NEW tcp dpt:22
5  REJECT        all  --  0.0.0.0/0              0.0.0.0/0                reject-with icmp-host-prohibited

Chain FORWARD (policy ACCEPT)
num target      prot opt source                destination              state
1  REJECT        all  --  0.0.0.0/0              0.0.0.0/0                reject-with icmp-host-prohibited

Chain OUTPUT (policy ACCEPT)
num target      prot opt source                destination
```

5. 执行如下命令，设置 IP 白名单，将回源 IP 段加入防火墙白名单中。

```
Iptables -A INPUT -s 回源IP -j ACCEPT
```

6. 执行如下命令，查看添加的白名单策略，是否成功添加到了防火墙配置中。

```
iptables -nL --line-number
```

如果看到添加的防火墙规则在输出内容内，则代表添加成功。

7. 执行如下命令，保存防火墙配置。

```
service iptables save
```

```
[root@localhost ~]# service iptables save
iptables: Saving firewall rules to /etc/sysconfig/iptables:[ OK ]
```

8. 执行如下命令，重启防火墙，使配置生效。

```
service iptables restart
```

```
[root@localhost /]# service iptables restart
iptables: Setting chains to policy ACCEPT: filter      [ OK ]
iptables: Flushing firewall rules:                    [ OK ]
iptables: Unloading modules:                          [ OK ]
iptables: Applying firewall rules:                    [ OK ]
```

原因二：处理步骤

将本地主机的解析结果修改为源站，来验证源站本身是否正常，首先修改本地 hosts 文件，具体操作如下：

1. 修改本地 hosts 文件，使本地对业务高防域名的请求到达源站 IP，下面以 Windows 操作系统为例，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：

<源站 IP 地址> <被防护网站的域名>

例如源站 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 文件中绑定的源站 IP 地址时，说明本地 hosts 生效。若没有解析到源站 IP，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 绑定已经生效之后，使用域名进行验证：源站是否可以正常访问，如不能正常访问，针对可能原因对应做如下处理。

处理措施1：源站 IP 保护

查看源站流量、请求量是否有大量增长，同时对比高防 IP 管理控制台中的监控。服务器本身流量监控以 CentOS 系统为例，具体操作如下：

1. 常见 Linux 服务器网络流量使用情况可以使用 iftop 进行查看：

执行命令：iftop [-i interface] (参数 -i 后跟的 interface 表示网络接口名，如 eth0、eth1)

输出如下：



回显结果说明：

- 第一行：带宽使用情况显示。
- 中间部分为外部连接列表，即记录了哪些 IP 正在和本机的网络连接。
- 中间部分靠右侧部分是实时流量信息，分别是该访问 IP 连接到本机2秒、10秒和40秒的平均流量。
- => 代表发送数据，<= 代表接收数据。
- 底部三行：
 - 第一列：TX 表示发送流量，RX 表示接收流量，TOTAL 表示总流量。
 - 第二列 cumm：表示第一列各种情况的总流量。
 - 第三列 peak：表示第一列各种情况的流量峰值。
 - 第四列 rates：表示第一列各种情况2秒、10秒、40秒内的平均流量。

2. 查看高防 IP 管理控制台的业务流量监控，参考 [防护概览（总览）](#)。

如果源站遭到大流量攻击，但高防IP管理控制台显示无异常，则有可能是攻击绕过高防IP直接攻击源站。此种源 IP 暴露的处理方法参考 [源站 IP 暴露的解决方法](#)。

处理措施2：请相关人员进行机房故障检查，修复物理故障

对服务器硬件状态进行自查：查看源站服务器机房是否出现断电、网卡、驱动、内存以及接线等物理硬件故障情况，及时更新或修复。

处理措施3：确认 Web 服务是否正常并修复

查看源站服务器的相关监控，CPU/内存的使用率、带宽的使用率等情况。

① 说明：

- 通常情况下 CPU 或者内存的使用率长时间超过90%，即可判断为状态异常。
- 带宽使用需要对比业务正常时期业务进程占用情况，查看是否有明显增长，可以参照 [云服务器带宽使用率过高](#)。

如有异常，进一步处理请您联系相关的技术人员或机房负责人员协助排查问题。

处理措施4：检查服务器进程占用，内存占用等性能参数是否正常并恢复至正常状态

对服务器 Web 程序状态进行自查：使用 `ps -C nginx -o pid` 命令查看服务器 nginx 进程是否正常运行。如有异常需要联系服务器技术人员，针对源站服务器中 Apache、Nginx 等服务进行修复至业务正常状态水平。

处理措施5：查看网络层面进行排查或者源站链路监控设备监控到的链路状态，也可通过更换链路测试进行验证与规避

对公网网络至源站服务器间链路质量，链路连通情况，中间网络设备转发情况等全面进行自查，确保此段链路连通性正常。

原因三：处理步骤

通过腾讯云拨测平台中的站点质量监控对源站 IP 和高防 IP 分别进行公网网络质量的检测和监控。监控方式可以参考 [腾讯云拨测使用说明](#)。

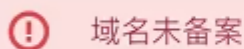
如果有公网网络质量不佳的情况，进一步需要联系所属运营商进行反馈处理。

域名接入高防 IP，提示未备案

最近更新时间：2024-04-23 14:52:01

现象描述

域名接入高防 IP，提示未备案。



可能原因

域名未在工信部备案

根据国务院令第292号《互联网信息服务管理办法》和《非经营性互联网信息服务备案管理办法》规定，国家对经营性互联网信息服务实行许可制度，对非经营性互联网信息服务实行备案制度。未获取许可或者未履行备案手续的，不得从事互联网信息服务，否则属于违法行为。

因此，所有对中国大陆境内提供服务的网站都必须先进行 ICP 备案，备案成功并获取通信管理局下发的 ICP 备案号后，才能开通访问。

备案信息未及时同步

若您接入域名已经在工信部备案成功，接入高防 IP 时提示域名未备案，可能是因为工信部备案信息还未同步腾讯云 ICP 备案系统。

处理步骤

域名未在工信部备案

您可以使用腾讯云 ICP 备案系统进行备案，备案成功并获取通信管理局下发的 ICP 备案号后，即可使用域名接入高防 IP。详情请参见：[备案概述](#)。

① 说明：

若您其他备案接入商进行备案，详情请咨询您的备案接入商。

备案信息未及时同步

备案完成后，一般工信部信息同步以及腾讯云备案管理系统的信息拉取均需要一定周期，请您等待24小时后再进行接入。

SDK 文档

水印 SDK

最近更新时间：2025-08-08 14:31:52

本文将为您介绍如何接入水印 SDK，本文主要包括 Android、iOS 和 Windows 三个版本的接入指南。

SDK 准备

下载相关 [Demo](#) 及 [SDK](#)。

Android 接入

预备工作

- 接入 SDK 需要完成以下步骤：
 - 1.1 根据运行平台选择相应的 so 文件，将 so 文件和 jar 文件拷贝到工程目录下并添加依赖。
 - 1.2 调用 SDK 接口函数，生成水印信息。
 - 1.3 发送报文时，将20字节水印信息放在消息体前面。
- SDK 文件包含 so 文件和 jar 文件，目录结构如下：



- SDK API 说明：
 - 程序包：com.gamesec
 - 类：Mark
- 接口说明：

接口名称	说明
CreateSDKBuffFromStr	生成水印

接入步骤（Android Studio）

1. 将 sdk/android 文件夹下的内容拷贝到工程目录的 libs 文件夹下:



2. 修改项目的 build.gradle 文件, 设置 jni 文件目录, 添加 jar 依赖:

```
android {
    sourceSets {
        main {
            jniLibs.srcDirs = ['libs/jni'] // 设置 jni 目录
        }
    }
    dependencies {
        implementation files('libs/gamesec.jar') // 添加依赖
    }
}
```

3. Eclipse 接入方法类似, 不需要配置 build.gradle 文件。

接口调用

1. 导入程序包。

```
import com.gamesec.*;
```

2. 实例化 Mark 对象。

```
Mark mark = new Mark();
```

3. 调用 CreateSDKBuffFromStr 生成水印。

```
byte [ ] CreateSDKBuffFromStr (String pSDKinfo, String buffer, String
uDesIp, int uDesPort)
```

● 参数说明:

参数	类型	含义
----	----	----

pSDKInfo	String	水印防护密钥
buffer	String	占位参数，传入空字符串即可
uDesIp	String	服务器 IP，如 “1.2.3.4”
uDesPort	int	服务器端口

- 返回值：

类型	含义
byte[]	计算的水印信息，取20字节

- 调用示例：

```
String pSDKInfo = "566c2dea9420eb37-b6c8-566c2dea9420eb3710525135e8485e80806a2f9c";
String uDesIp = "115.159.147.198";
int uDesPort = 8899 ;
byte[] bytes = mark.CreateSDKBuffFromStr(pSDKInfo, "", uDesIp, uDesPort);
```

4. 添加水印信息到消息体。代码示例如下：

```
Socket s = new Socket(uDesIp, uDesPort);
OutputStream out = s.getOutputStream();
PrintWriter output = new PrintWriter(out, true);
// 先传入水印信息
output.print(bytes);
output.println("msg msg msg");
BufferedReader input = new BufferedReader(new
InputStreamReader(s.getInputStream()));
String msg = input.readLine();
s.close();
```

iOS 接入

预备工作

- 接入 SDK 需要完成以下步骤：

1.1 将 SDK 文件拷贝到工程目录，Swift 工程需要添加桥文件。

1.2 调用 SDK 接口函数，生成水印信息。

1.3 发送报文时，将 20 字节水印信息放在消息体前面。

- SDK 文件包含 a 文件和 h 文件，目录结构如下：

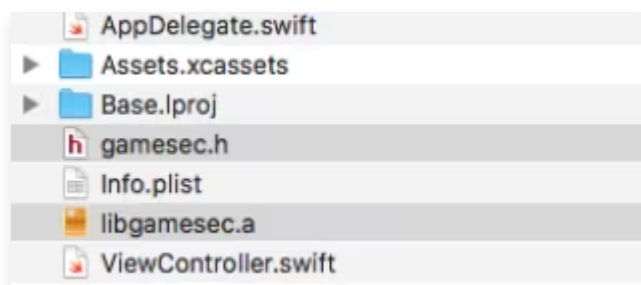


- 接口说明：

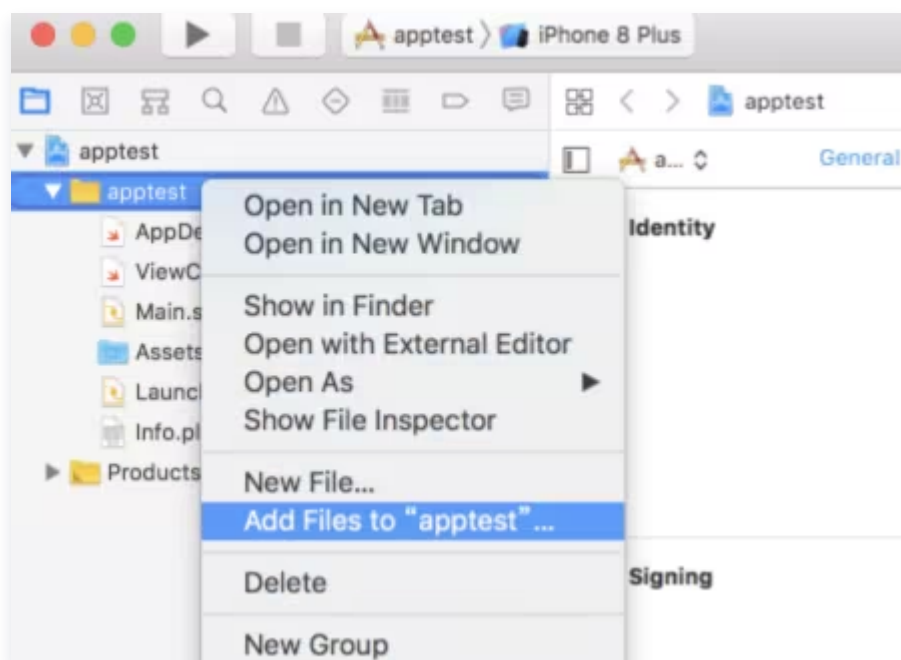
接口名称	说明
CreateSDKBuffFromStr	生成水印

接入步骤（Xcode）

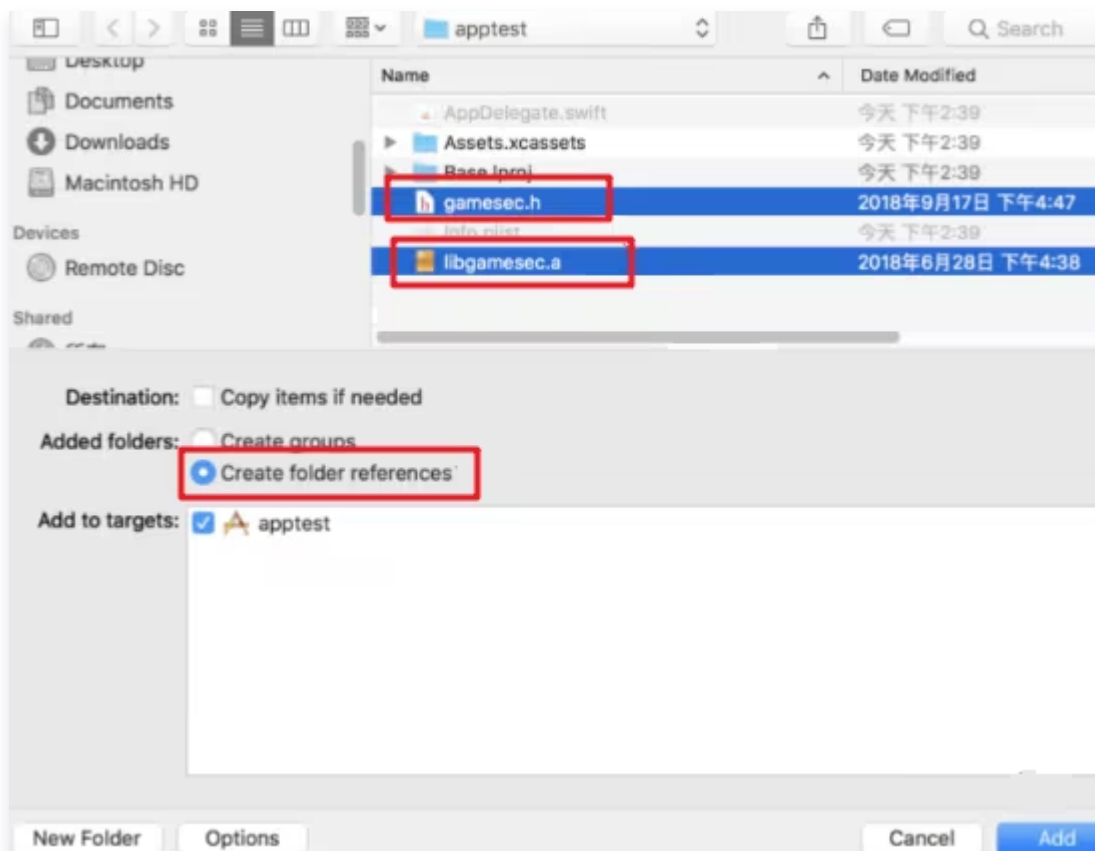
- 将 sdk/ios 文件夹下的内容拷贝到工程目录：



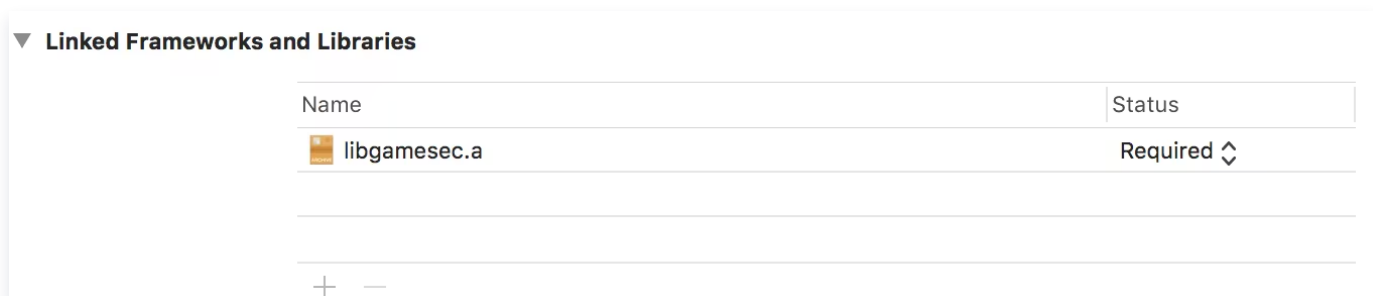
- 将 SDK 文件添加到 Xcode。右键工程名，单击 “Add Files to”。



3. 在对话框中勾选 “Create folder references”，选中 SDK 的两个文件，单击 **Add**。



4. 左键工程名，选择 General，将 a 文件添加到 “Linked Frameworks and Libraries”：

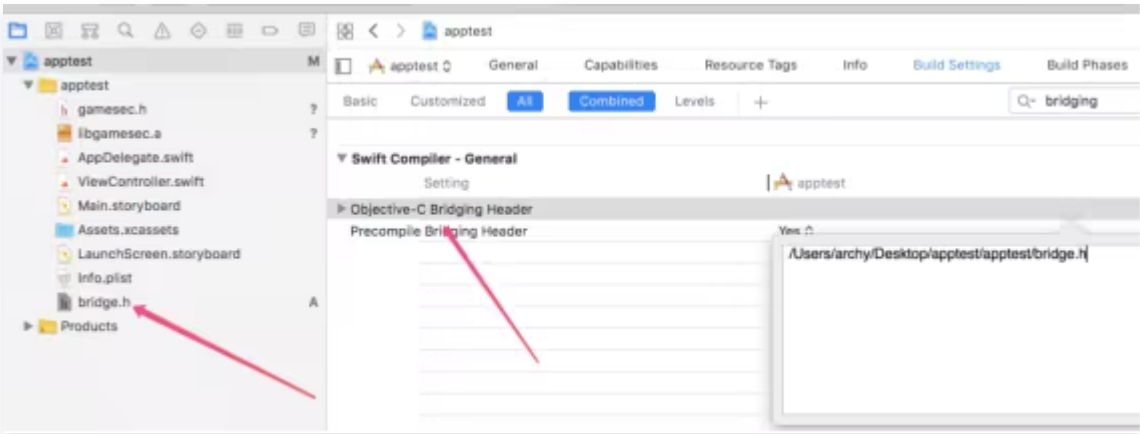


5. 如果是 Swift 项目，需要创建桥文件，Objective-C 项目可以跳过此步骤。创建一个 Header File，命名为 bridge.h。并在文件中添加以下代码：

```
# import "gamesec.h";
```

6. 左键工程名，选择 Build Settings，将 bridge.h 添加到 Objective-C Bridging Header 中：

7.



接口调用

1. Swift 项目可以直接调用生成水印函数，Objective-C 项目需要在使用的文件里面添加头文件：

```
# import "gamesec.h";
```

2. 调用 CreateSDKBuffFromStr 生成水印。

```
uint32_t CreateSDKBuffFromStr(char *pSDKInfo, uint8_t *buffer, char*
uDstIp, uint16_tuDstPort);
```

参数说明：

参数	类型	含义
pSDKInfo	char *	水印防护密钥
buffer	uint8_t *	水印指针，输出水印结果
uDesIp	char *	服务器 IP，如 “1.2.3.4”
uDesPort	uint16_t	服务器端口

① 注意：

水印结果保存在参数 buffer 中，取20字节。

3. 调用示例。

```
Swift 调用：
let pSDKInfo = UnsafeMutablePointer<Int8>(mutating: (
```

```
        "566c2dea9420eb37-b6c8-  
566c2dea9420eb3710525135e8485e80806a2f9c"  
        as NSString).utf8String);  
        var buffer =  
UnsafeMutablePointer<UInt8>.allocate(capacity: 20);  
        let uDstIp = UnsafeMutablePointer<Int8>(mutating: (  
        "115.159.147.198" as NSString).utf8String);  
        let uDstport = UInt16.init("8899")!;  
  
        CreateSDKBuffFromStr(pSDKInfo, buffer, uDstIp,  
uDstport);  
  
        for i in 0 ..< 20 {  
            let b = (buffer+i).pointee;  
            // 水印信息在前20字节, 注意这里输出的是  
uint8  
            print(" \ (b) ");  
        }  
    }
```

Object-C 调用:

```
        char *pSDKInfo = "566c2dea9420eb37-b6c8-  
566c2dea9420eb3710525135e8485e80806a2f9c";  
        uint8_t buffer[20];  
        char *uDstIp = "115.159.147.198";  
        uint16_t uDstPort = 8899;  
  
        CreateSDKBuffFromStr(pSDKInfo, buffer, uDstIp,  
uDstPort);  
  
        for(int i=0;i<20;i++)  
        {  
            // 水印信息在前20字节  
            NSLog(@"%d", (int8_t)buffer[i]);  
        }  
    }
```

3. 发送报文前, 添加 20 字节水印信息到消息体前面。

Windows 接入

预备工作

SDK 为 gamesec.dll 文件，有一个生成水印的函数：

```
uint32_t CreateSDKBuffFromStr(char *pSDKInfo, uint8_t *buffer, char*
uDstIp, uint16_t uDstPort);
```

参数说明：

参数	类型	含义
pSDKInfo	char *	水印防护密钥
buffer	uint8_t *	水印指针，输出水印结果
uDesIp	char *	服务器 IP，如 “1.2.3.4”
uDesPort	uint16_t	服务器端口

❗ 注意：

水印结果保存在参数 buffer 中，取20字节。

接口调用

在使用水印函数时，需先导入 dll 文件，可以使用 LoadLibrary 函数（需要添加 Windows.h ）：

```
// 定义函数指针
typedef int(*FUNC)(char *, uint8_t *, char* , uint16_t );
// 设置 dll 路径
HINSTANCE Hint = ::LoadLibrary(L"E:\\sdk\\gamesec.dll");
FUNC CreateSDKBuffFromStr = (FUNC)GetProcAddress(Hint,
"CreateSDKBuffFromStr");
```

完整调用示例：

```
// 保存水印
uint8_t buffer[BUFFER_SIZE];
memset(buffer, 0, BUFFER_SIZE);

int UDP_TEST_PORT = 8899;

const char * CONST_UDP_SERVER_IP = "115.159.147.198";
char * UDP_SERVER_IP = new char[strlen(CONST_UDP_SERVER_IP)];
```

```
strcpy(UDP_SERVER_IP, CONST_UDP_SERVER_IP);

const char * CONST_pSDKinfo =
"566c2dea9420eb37-b6c8-566c2dea9420eb3710525135e8485e80806a2f9c";
char * pSDKinfo = new char[strlen(CONST_pSDKinfo)];
strcpy(pSDKinfo, CONST_pSDKinfo);

// 调用10次
for (int i = 0; i < 5; i++) {
    CreateSDKBuffFromStr(pSDKinfo, buffer, (char *)UDP_SERVER_IP,
UDP_TEST_PORT);

    for (int i = 0; i <= 20; i++)
    {
        // 水印在前20字节
        printf("%d ", (int8_t)buffer[i]);
    }
    printf("\n\n");
}
```

水印 SDK 个人信息保护规则

最近更新时间：2023-07-21 09:44:33

引言

DDoS 防护——水印 SDK(以下简称“SDK 产品”)由腾讯云计算(北京)有限责任公司(以下简称“我们”)开发,公司注册地为北京市海淀区知春路49号3层西部309。

我们在此特别声明:

1. 本 SDK 产品功能的实现将不需要收集、获取、传输、分享或者使用终端用户的任何个人信息。
2. 我们不会因为开发者适配、集成和装载本 SDK 产品而向其提供、传输或共享任何的个人信息。
3. 如果开发者因提供其产品或服务而需要处理终端用户的个人信息,由开发者独自承担相应的法律责任。
4. 请终端用户注意,在开发者将本 SDK 产品适配、集成或装载到开发者产品或服务前,我们已经要求相关开发者仔细阅读我们在官网公示的相关服务协议、本规则及开发者合规指南(或具有同样性质的相关法律文件),并已经要求开发者依据开发者的产品收集使用个人信息的情况进行合规自查。
5. 如果我们更新、改进或修改了本 SDK 产品,并因此导致我们需要处理终端用户的个人信息的,我们将会依据适用法律的要求对本规则进行修订,并将修订后的内容及时告知开发者和终端用户,我们将要求开发者适时更新其隐私政策,并以弹框形式通知终端用户并且获得其同意。
6. 对于本规则的任何内容存在疑问的,可以通过如下的方式与我们取得联系:
 - (1) 通过 <https://kf.qq.com/> 与我们联系进行在线咨询。
 - (2) 发送邮件至: Dataprivacy@tencent.com。
 - (3) 邮寄信件至: 中国广东省深圳市南山区海天二路33号腾讯滨海大厦,数据隐私保护部(收),邮编: 518054。

DDoS 高防包（旧版）

产品简介

产品概述

最近更新时间：2025-08-07 15:13:21

简介

DDoS 高防包是针对业务部署在腾讯云内的用户提升 DDoS 防护能力的付费产品。DDoS 高防包直接对腾讯云上 IP 生效，无需更换 IP，购买后只需绑定需要防护的 IP 即可使用，具备接入便捷、零变更等特点。DDoS 高防包支持为 IPv6 和 IPv4 两种类型的 IP 提供防护，同时支持单 IP 防护，也提供多 IP 共享防护资源功能，满足多个 IP 地址都需要提升防护能力的需求。

腾讯云 DDoS 高防包提供独享包与共享包两种类型的高防包，用户可根据需求自行选择：

- 独享包：提供一个 IP 独享防护能力。
- 共享包：提供多个 IP 共享防护能力。

主要功能

多类型防护

防护分类	描述
畸形报文过滤	过滤 frag flood，smurf，stream flood，land flood 攻击，过滤 IP 畸形包、TCP 畸形包、UDP 畸形包
网络层 DDoS 攻击防护	过滤 UDP Flood、SYN Flood、TCP Flood、ICMP Flood、ACK Flood、FIN Flood、RST Flood、DNS/NTP/SSDP 等反射攻击、空连接
应用层 DDoS 攻击防护	过滤 CC 攻击和 HTTP 慢速攻击，支持 HTTP 自定义特征过滤如 host 过滤、user-agent 过滤、referer 过滤

防护对象可切换

DDoS 高防包支持单 IP，也支持多个 IP 共享防护资源，满足各种业务场景。用户可根据业务需要，切换防护对象，支持切换的对象包括 CVM、CLB、WAF、NAT 网关等。

高级安全策略灵活

DDoS 高防包默认提供基础安全策略，策略基于 IP 画像、行为模式分析、AI 智能识别等防护算法，有效应对常见 DDoS 攻击行为。同时提供 DDoS 高级防护策略，用户可根据特殊业务特点灵活设置，应对不断变化的攻击手法。

防护统计及分析

DDoS 高防包提供实时详细的流量报表及攻击防护详细信息，便于用户及时、准确了解 DDoS 高防包的防护效果。同时支持攻击取证，可对攻击情况进行抓包下载，方便快速分析异常问题以及溯源。

产品优势

最近更新时间：2025-08-07 15:13:21

DDoS 高防包是一键为腾讯云内 CVM、CLB、NAT 网关等云产品提升 DDoS 防护能力的付费服务，其产品优势如下：

一键接入，无需任何业务变更

无需进行业务变更，接入配置便捷，购买 DDoS 高防包后，只需绑定需要防护的云产品的 IP 地址即可使用，只需几分钟即可生效。

超大防护资源

采用 BGP 防护带宽，可为单用户单点提供高达300Gbps的 DDoS 防护能力，轻松抵御 DDoS 攻击，满足活动大促、活动上线等重要业务的安全稳定性保障需求。

领先的清洗能力

依托腾讯自研防护集群，采用 IP 画像、行为分析、Cookie 挑战等多维算法，并通过 AI 智能引擎持续更新防护算法，精准快速检测业务流量，灵活应对各类攻击行为。

极速访问体验

腾讯云 BGP 链路对接全国各地30家运营商，覆盖面广，能有效解决访问时延问题，保障各类用户群的访问速度，带来极速访问体验。

支持双协议防护

DDoS 高防包支持同时为 IPv6 和 IPv4 两种类型的 IP 提供防护，满足客户对 IPv6 类型服务器需要防护的需求，无需额外购买或升级高防包，只需绑定需要防护的云产品的 IP 地址后即可实现 DDoS 防护。

定价灵活，优化成本

提供“保底防护+弹性防护”相结合计费方式，为用户降低日常安全费用，在需要时按需调整弹性防护，无需新增任何设备，无需调整配置。当攻击流量超过保底防护峰值时，腾讯云仍为用户继续防护，保障业务不中断，按当天实际攻击量付费。

丰富的攻击防护报表

提供精准的防护流量报表及攻击详情信息，使用户及时了解攻击实况。支持对攻击自动抓包，方便事后进行分析以及溯源。

应用场景

最近更新时间：2023-07-21 09:44:34

游戏

游戏行业是 DDoS 攻击的重灾区，DDoS 高防包能有效保证游戏的可用性和持续性，保障游戏玩家流畅体验，同时为活动、新游戏发布或节假日游戏收入旺季时段保驾护航，确保游戏业务正常。

互联网

保证互联网网页的流畅访问，业务正常不中断，对电商大促等重大活动时段，提供安全护航。

金融

满足金融行业的合规性要求，保证线上交易的实时性及安全稳定性。

政府

满足国家政务云建设标准的安全需求，为重大会议、活动、敏感时期提供安全保障，保障民生服务正常可用，维护政府公信力。

企业

保障企业站点服务持续可用，避免 DDoS 攻击带来的经济及企业品牌形象损失问题，零硬件零维护，节省安全成本。

相关概念

最近更新时间：2023-07-27 11:17:12

DDoS 攻击

Distributed Denial of Service (DDoS)，即分布式拒绝服务攻击，是指攻击者通过网络远程控制大量僵尸主机向一个或多个目标发送大量攻击请求，堵塞目标服务器的网络带宽或耗尽目标服务器的系统资源，导致其无法响应正常的服务请求。

网络层 DDoS 攻击

网络层 DDoS 攻击主要是指攻击者利用大流量攻击拥塞目标服务器的网络带宽，消耗服务器系统层资源，导致目标服务器无法正常响应客户访问的攻击方式。

常见攻击类型包括 SYN Flood、ACK Flood、UDP Flood、ICMP Flood 以及 DNS/NTP/SSDP/memcached 反射型攻击。

CC 攻击

CC 攻击主要是指通过恶意占用目标服务器应用层资源，消耗处理性能，导致其无法正常提供服务的攻击方式。

常见的攻击类型包括基于 HTTP/HTTPS 的 GET/POST Flood、四层 CC 以及 Connection Flood 等攻击方式。

防护峰值

防护峰值分为保底防护峰值和弹性防护峰值。

- 保底防护峰值：指高防服务实例的保底防护带宽能力，保底部分为按月预付费。
- 弹性防护峰值：指高防服务实例的最大弹性防护带宽能力，弹性部分为按天后付费。

若未开启弹性防护，则保底防护峰值为高防服务实例的最高防护峰值。若已开启弹性防护，则弹性防护峰值作为高防服务实例的最高防护峰值。当攻击流量超过高防服务实例的最高防护峰值后触发封堵。

① 说明：

弹性防护默认关闭。如需开启弹性防护，请在知悉弹性相关收费后自主开启。用户可以根据自身业务需求，随时调整弹性防护峰值。

弹性防护峰值的作用

开启弹性防护后，当攻击流量峰值超过购买的保底防护峰值且在弹性防护峰值范围内时，腾讯云 DDoS 高防包可继续为用户提供防护，保障业务访问持续性。

弹性防护如何收费

开启弹性防护后，当攻击流量超过保底防护峰值时，会触发弹性防护并收取费用，取当天实际产生的最高攻击峰值所对应区间进行计费，账单次日生成。

例如，您购买的保底防护为20Gbps，且设置的弹性防护为50Gbps。若当天的实际攻击峰值为35Gbps，则需要支付30Gbps – 40Gbps区间的弹性防护费用。

详细费用请参见 [计费概述](#)。

清洗

当目标 IP 的公网网络流量超过设定的防护阈值时，腾讯云 DDoS 防护系统将自动对该 IP 的公网入向流量进行清洗。通过 DDoS 路由协议将流量从原始网络路径中重定向到DDoS 防护系统的 DDoS 清洗设备上，通过清洗设备对该 IP 的流量进行识别，丢弃攻击流量，将正常流量转发至目标 IP。

通常情况下，清洗不会影响正常访问，仅在特殊场景或清洗策略配置有误时，可能会对正常访问造成影响。

封堵

当目标 IP 受到的攻击流量超过其封堵阈值时，腾讯云将通过运营商的服务屏蔽该 IP 的所有外网访问，保护云平台其他用户免受影响。简而言之，当您的某个 IP 受到的攻击流量超过您所购买的高防套餐最大 [防护峰值](#) 时，腾讯云将屏蔽该 IP 的所有外网访问。当您的防护 IP 被封堵时，您可以登录管理控制台 [自助解封](#)。

封堵阈值

DDoS 高防包实例的防护 IP 的封堵阈值等于实际购买的最大 [防护峰值](#)。DDoS 高防包有多种不同规格，详情请参考 [计费概述](#)。

封堵时长

封堵时长默认为2小时，实际封堵时长与当日封堵触发次数和攻击峰值相关，最长可达24小时。

封堵时长主要受以下因素影响：

- 攻击是否持续。若攻击一直持续，封堵时间会延长，封堵时间从延长时刻开始重新计算。
- 攻击是否频繁。被频繁攻击的用户被持续攻击的概率较大，封堵时间会自动延长。
- 攻击流量大小。被超大型流量攻击的用户，封堵时间会自动延长。

① 注意：

针对个别封堵过于频繁的用户，腾讯云保留延长封堵时长和降低封堵阈值的权利。

为什么进行封堵

腾讯云通过共享基础设施的方式降低用云成本，所有用户共享腾讯云的外网出口。当发生大流量攻击时，除了会影响被攻击对象，整个腾讯云的网路都可能会受到影响。为了避免攻击影响到其他未被攻击的用户，保障整个云平台网络的稳定，需要进行封堵。

为什么不提供免费无限抗攻击

DDoS 攻击不仅影响受害者，也会对整个云网络造成严重影响，影响云内其它未被攻击的用户。DDoS 防御的成本非常高，一是带宽成本，二是清洗成本。其中最大的成本就是带宽费用，带宽费用以总流量计算，不会考虑是正常流量或是攻击流量而区别收费。

因此，腾讯云在成本可承受的范围内为云服务用户提供免费的 DDoS 基础防护服务，当攻击流量超出免费防护阈值时，腾讯云会屏蔽被攻击 IP 的外网流量。

有关封堵的更多信息，请参见 [封堵相关问题](#)。

相关产品

最近更新时间：2026-03-17 10:47:31

使用 DDoS 高防包可为如下产品提升 DDoS 防护能力：

- **云服务器**：是腾讯云提供的可扩展的计算服务。使用云服务器 CVM 避免了使用传统服务器时需要预估资源用量及前期投入的问题，帮助您在短时间内快速启动任意数量的云服务器并即时部署应用程序。
- **负载均衡**：提供安全快捷的流量分发服务，访问流量经由 CLB 可以自动分配到云中的多台云服务器上，扩展系统的服务能力并消除单点故障。
- **Web 应用防火墙**：是一款基于 AI 的一站式 Web 业务运营风险防护方案。
- **NAT 网关**：是一种支持 IP 地址转换服务，提供 SNAT 和 DNAT 能力，可为私有网络（VPC）内的资源提供安全、高性能的 Internet 访问服务。
- **VPN 连接**：是一种基于网络隧道技术，实现本地数据中心与腾讯云上资源连通的传输服务，它能帮您在 Internet 上快速构建一条安全、可靠的加密通道。
- **裸金属云服务器**：是一种可按需购买、按量付费的物理服务器租赁服务，提供给您云端专用的高性能、安全隔离的物理服务器集群。
- **全球应用加速**：全球应用加速（Global Application Acceleration Platform，GAAP）依赖全球节点之间的高速通道、转发集群及智能路由技术，实现各地用户的就近接入，通过高速通道直达源站区域，帮助业务解决全球用户访问卡顿或者延迟过高的问题。
- **弹性网卡**：是绑定私有网络（Virtual Private Cloud，VPC）内云服务器的一种弹性网络接口，可在多个云服务器间自由迁移。弹性网卡对配置管理网络与搭建高可靠网络方案有较大帮助。

购买指南

计费概述

最近更新时间：2025-06-10 09:29:22

目前 DDoS 高防包支持购买的区域：华北（北京）、华东（上海）、华南（广州）。

计费方式

DDoS 高防包的计费方式为“保底防护峰值（预付费）+弹性防护峰值（后付费）”。

计费项	计费模式	付费方式	付费说明
保底防护峰值	包年包月	预付费	提供基础防护带宽，预付费价格由保底防护峰值和购买时长确定。若升级保底防护，则在原有的基础上加收额外费用，且防护级别只可升不可降。
弹性防护峰值	按天按量计费	后付费	触发弹性防护后，按当天最高攻击峰值所对应的弹性防护峰值区间计费，账单次日生成。若未触发弹性防护，则不收取任何费用。 支持升级、降级配置。

产品价格

百 G 包年套餐

百 G 包年套餐

DDoS 防护能力	CC 防护能力	单价（元/年）
100Gbps	300,000QPS	328,000
200Gbps	500,000QPS	358,000
300Gbps	700,000QPS	368,000

i 说明：

- 百 G 包年套餐仅限中国内地（大陆）区域售卖。
- DDoS 防护能力为100Gbps的包年套餐，弹性防护峰值可以配置到300Gbps。弹性相关收费请参见[弹性防护区间价格](#)。
- 支持对百 G 包年套餐进行按月续费，例如，100Gbps包年套餐32.8万元，续费2个月，则大致需要5.47（32.8/12*2）万元。

- 建议选择最靠近业务源站的地域，可降低访问时延，提高访问速度。

保底防护

保底防护按月预付费，具体价格请参考如下表格：

类型	保底防护峰值	防护 IP 个数	CC 防护峰值	单价（元/月）
独享包	5Gbps	1	10,000QPS	100
	20Gbps		40,000QPS	6,000
	30Gbps		70,000QPS	16,600
	50Gbps		150,000QPS	25,600
共享包	20Gbps	5	40,000QPS	17,600
		10		29,800
		20		52,800
		50		118,800
		100		198,000
	50Gbps	5	150,000QPS	64,600
		10		119,800
		20		201,800
		50		462,000
		100		739,200
	100Gbps	5	300,000QPS	168,000
		10		208,000
		20		568,000
		50		880,000
		100		1,000,000

说明：

- Query Per Second（QPS），此处用于衡量 DDoS 高防包实例每秒可防护的 CC 攻击请求数。

- 购买并绑定高防包后，被绑定 IP 仅具有购买的高防包的防护能力，不叠加基础防护。
- 保底防护峰值为20Gbps/30Gbps/50Gbps的独享包，不支持升级为100Gbps及以上的保底防护规格，最大支持升级为50Gbps。

弹性防护

用户可根据实际业务防护需求自助开启弹性防护。

- 未开启弹性防护时，最高防护峰值为保底防护峰值且不会产生后付费。
- 开启弹性防护时，弹性防护峰值为实例的最高防护峰值。
 - 未触发弹性防护时，不产生费用。
 - 当触发弹性防护（攻击峰值超过保底防护峰值且在弹性防护范围内）时，取当天实际发生的最高攻击峰值所对应计费区间进行计费，账单次日生成。

弹性防护具体价格请参考如下表格：

DDoS 防护峰值	单价（元/天）
20Gbps ≤ 攻击峰值 < 30Gbps	3,500
30Gbps ≤ 攻击峰值 < 40Gbps	4,800
40Gbps ≤ 攻击峰值 < 50Gbps	5,700
50Gbps ≤ 攻击峰值 < 60Gbps	6,600
60Gbps ≤ 攻击峰值 < 70Gbps	7,500
70Gbps ≤ 攻击峰值 < 80Gbps	8,350
80Gbps ≤ 攻击峰值 < 90Gbps	9,200
90Gbps ≤ 攻击峰值 < 100Gbps	10,050
100Gbps ≤ 攻击峰值 < 120Gbps	11,750
120Gbps ≤ 攻击峰值 < 150Gbps	14,300
150Gbps ≤ 攻击峰值 < 200Gbps	18,550
200Gbps ≤ 攻击峰值 < 250Gbps	22,800
250Gbps ≤ 攻击峰值 < 300Gbps	26,800

计费示例

DDoS 高防包使用组合计费方式，计费示例说明如下：

- **独享包费用计算示例**

例：用户在上海区域购买了一个独享包，规格是“20Gbps保底防护峰值 + 50Gbps弹性防护峰值”。

若当天发生 DDoS 攻击事件且最高攻击流量峰值为45Gbps，超过保底防护峰值范围且使用了弹性防护峰值，落入 $40\text{Gbps} < \text{弹性峰值} \leq 50\text{Gbps}$ 计费区间，当天产生弹性费用5700元。

则用户需支付费用合计为11700元，其中包含当月的保底防护费用6000元，当天产生的弹性费用5700元。

- **共享包计算示例**

例：用户在上海区域购买了一个共享包，规格是“20Gbps保底防护峰值 + 80Gbps弹性防护峰值，IP 数量5个”。

若当天发生多个 IP 同时被攻击的事件，有3个 IP 同时受到攻击攻击流量分别为10Gbps、15Gbps和30Gbps。则同时遭受攻击的叠加峰值为 $10 + 15 + 30 = 55\text{Gbps}$ ，超过了20Gbps的保底防护峰值且使用了弹性防护峰值，落到了 $50\text{Gbps} < \text{弹性峰值} \leq 60\text{Gbps}$ 计费区间，当天产生弹性费用6600元。

则用户需支付费用合计为24200元，其中包含当月的保底防护费用17600元，当天产生的弹性费用6600元。

购买指引

最近更新时间：2023-07-21 09:44:35

前提条件

在购买 DDoS 高防包实例前，您需要完成 [注册腾讯云](#) 账号，并完成 [实名认证](#)。

操作步骤

1. 登录腾讯云官网，进入 DDoS 高防包购买页，购买产品。

① 注意：

目前已不支持购买旧版 DDoS 高防包，如需购买 DDoS 高防包，可参见新版 DDoS 高防包 [购买指引](#) 进行购买。

2. 根据实际需求配置如下参数。

① 说明：

以下参数仅针对旧版 DDoS 高防包购买页进行说明。

- 套餐：选择**独享包**或**共享包**。
 - 独享包可以绑定一个腾讯云公网 IP，该 IP 独享防护能力。
 - 共享包可以绑定多个腾讯云公网 IP，且多个 IP 共享防护能力。
- （可选）IP 数量：仅当套餐设置为**共享包**时，该参数可见。表示高防包可绑定的腾讯云公网 IP 数量。
- 地域：请选择腾讯云源站服务器所在地域，DDoS 高防包目前仅支持为同区域的腾讯云公网 IP 提供高防服务。
- 保底防护峰值：按包年包月预付费。建议以历史攻击流量的平均值为参考，选择的保底防护峰值略高于平均值，以便足够防御大部分攻击行为。
- 购买个数：设置需要购买的实例数量，单次操作最多购买100个 DDoS 高防包实例。
- 购买时长：设置需要购买的时长，将根据 IP 数量、保底防护峰值以及购买时长计算需要预付的费用。
- 自动续费：用户可自行勾选。开启自动续费后，在腾讯云账号余额充足情况下，服务到期后将按月自动续费，保障业务防护不中断。
- 弹性防护峰值：按实际防护量计费，每日结算。建议以历史最高攻击流量为参考，选择的弹性防护峰值略高于历史最高峰值，以便足够防御大流量攻击，避免超过防护峰值而引起的 IP 封堵。

套餐

独享包

共享包

DDoS高防独享包可以绑定腾讯云服务器或负载均衡的一个公网IP上，绑定的IP专享防护峰值
DDoS高防共享包可以绑定腾讯云服务器或负载均衡的多个公网IP上，绑定的多IP共享防护峰值。若多IP同时遭受攻击，当叠加峰值超过防护峰值时，从攻击流量最大的IP地址开始封堵

地域

华南地区

华东地区

华北地区

广州

上海

北京

该高防包只能绑定广州地区的云主机或负载均衡

保底防护峰值

5Gbps

20Gbps

30Gbps

50Gbps

此部分为预付费，需按您当前选择的计费模式支付，如果想提升防御可选择提升弹性防护带宽，根据实际攻击按天计费

CC防护峰值

40,000QPS

计费模式

包年包月

购买个数

-

1

+

一次最多购买100个

购买时长

1个月

2个月

3个月

4个月

5个月

6个月

7个月

8个月

9个月

1年

2年

3年

自动续费

☐ 账户余额足够时，设备到期后按月自动续费

弹性防护峰值

无

30Gbps

40Gbps

50Gbps

60Gbps

70Gbps

80Gbps

90Gbps

100Gbps

运营骨干线路故障或其他运营策略等不确定因素，可能会造成未达到弹性上限发生封禁。如果发生未达开通的弹性峰值上限产生封禁的情况，免除当日弹性防护费用。
实际的DDoS防护能力为30Gbps，如果攻击发生当日流量峰值超出保底防护带宽，会按照当日流量峰值落入的计费区间进行计算，产生后付费账单。具体可参考[产品价格详情](#)

3. 单击立即支付，完成支付流程。

更多信息

- DDoS 高防包详细计费说明
- 计费相关常见问题

续费指引

最近更新时间：2023-07-21 09:44:35

为能继续享受正常的安全服务，用户可以在 DDoS 高防包服务到期前为其手动续费，也可以设置到期自动续费。

续费提醒

DDoS 高防包服务到期前7天，系统会向您推送服务即将到期、请及时续费等相关信息，信息通过站内信、短信及邮件的方式通知到腾讯云账号创建者以及所有协作者。具体详情请参考 [欠费说明](#)。

在 [购买 DDoS 高防包](#) 时，若已勾选并同意自动续费。在实例到期前，系统会向您发送提醒信息并自动生成续费订单，无需手动续费。

购买时长	☒ 1个月	☐ 2个月	☐ 3个月	☐ 4个月	☐ 5个月	☐ 6个月	☐ 7个月	☐ 8个月	☐ 9个月	☐ 1年	☐ 2年	☐ 3年
自动续费	☒ 账户余额足够时，设备到期后按月自动续费											

① 说明：

按月或按年开通的 DDoS 高防包实例，其自动续费周期都为3个月。

续费方式

控制台续费

1. 登录 [DDoS 防护管理控制台](#)。
2. 选择 [DDoS 高防包](#) > [资产列表](#)，单击目标实例操作列中的[续费](#)。
3. 在续费页面选择[续费时长](#)，并完成相关支付流程。

续费管理中心续费

在 [续费管理页面](#) 提供实例的批量资源续费、设置自动续费、设置统一到期日以及取消不续费等功能，详见 [续费管理](#)。

欠费说明

最近更新时间：2023-07-21 09:44:35

包年包月资源

到期提醒

对于包年包月的云资源服务，DDoS 高防包系统会在到期前的7天内，向用户推送“服务即将到期，请及时续费”等相关信息，信息通过站内信、短信、邮件或微信的方式，通知到腾讯云账号创建者以及所有协作者。

续费提醒

DDoS 高防包实例在到期前7天内，系统会给腾讯云账号的创建者以及所有协作者发送续费提醒通知。

① 注意：

在账户余额充足的情况下，若用户已设置自动续费，系统会在到期当日自动续费。

回收机制

独享型高防包

- 服务资源到期前7天内，系统开始给用户发送续费提醒通知。
- 到期之日起24小时内，服务仍可以继续使用，系统将发送服务已到期提醒通知，期间用户可以进行续费，并继续享受防护服务。
- 到期之日起24小时后，服务不可用，此实例将被系统回收，配置数据将被清除且不可恢复，DDoS 防护将恢复到免费的2Gbps防护能力（VIP 用户10Gbps）。

共享型高防包

- 服务资源到期前7天，系统开始给用户发送续费提醒通知。
- 到期后7天内，服务可以继续使用，系统将发送服务已到期提醒通知。
- 到期后第8天零点，实例进入回收站保留7天，期间服务不可用，用户仍可以通过续费找回数据并继续享受防护服务。
- 若用户未进行续费，在第15天零点，此实例将被系统回收，配置数据将被清除且不可恢复，DDoS 防护将恢复到免费的2Gbps防护能力（VIP 用户10Gbps）。

按量计费资源

欠费提醒

DDoS 高防包系统会在每个整点对按量计费资源进行扣费。当您的账户被扣为负值时，系统将通过站内信、短信、邮件或微信的方式，通知到腾讯云账户的创建者以及所有协作者。

① 注意：

欠费提醒功能默认关闭。如您的账户开通了按量计费的资源，为了让您预知账户即将欠费，预留一定的时间及时充值或备份数据，以保证云资源的正常使用，建议您前往腾讯云控制台 > 费用中心 > 主页 > [费用预警](#) 进行订阅。详细信息请参见 [余额预警指引](#)。

欠费处理

当您的账户余额被扣为负值时，DDoS 高防包服务的弹性防护能力将会被关闭，但未到期的按月预付费保底防护能力不受影响。在您的包年包月云资源有效期内，当您的账户余额为正值时，弹性防护能力将会自动恢复至欠费前所设置的弹性防护峰值。

退费说明

最近更新时间：2023-07-21 09:44:35

腾讯云 DDoS 高防包服务不支持提前退订，不适用五天无理由退款。若您已购买 DDoS 高防实例，则不支持退款。

快速入门

最近更新时间：2023-07-21 09:44:35

DDoS 高防包为腾讯云公网 IP 提供更高的 DDoS 防护能力，可支持防护 CVM、CLB、NAT、WAF 等产品和服务。DDoS 高防包接入便捷，无需变更业务 IP，可快速完成防护配置。

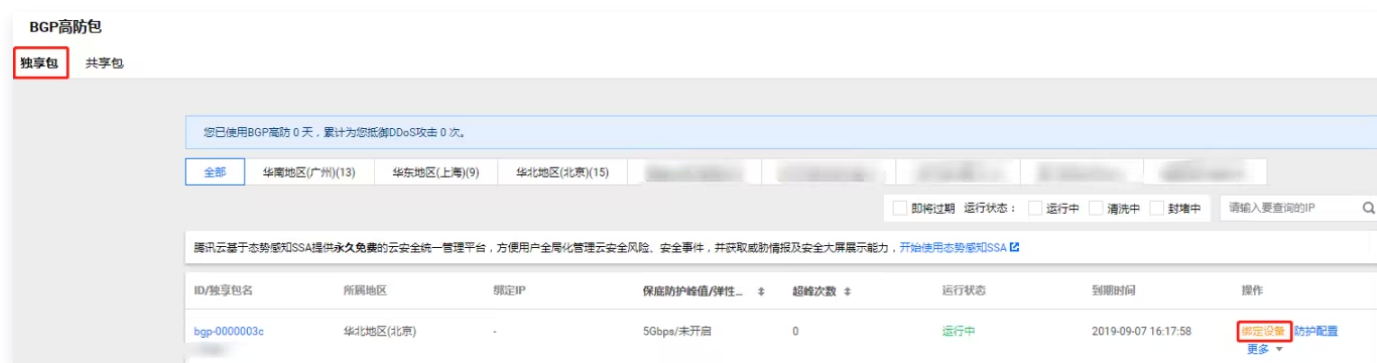
目前，腾讯云 DDoS 高防包提供独享包与共享包两种类型的高防包。

前提条件

在绑定防护 IP 前，您需要成功 [购买 DDoS 高防包实例](#)。

操作步骤

1. 登录 [DDoS 防护管理控制台](#)，前往 **DDoS 高防包 > 资产列表**。
 - 若您的 DDoS 高防包实例是独享包，则选择**独享包**页签。
 - 若您的 DDoS 高防包实例是共享包，则选择**共享包**页签。
2. 选择目的高防包实例所在地域，单击目的高防包实例所在行的操作项**绑定设备**。



3. 在绑定设备页面，根据实际防护需求选择**关联设备类型**与**选择关联机器**。

- 若您的 DDoS 高防包实例是独享包，仅支持绑定一个关联机器。

绑定设备

ID/服务包名

bgp-000005v_

地域

华东地区(上海)

已绑定设备

关联设备类型

☒ 云主机

☐ 负载均衡

☐ 黑石物理机

☐ 黑石负载均衡

☐ Web应用防火墙

☐ NAT网关

☐ VPN网关

☐ 弹性网卡

☐ GAAP

☐ 黑石弹性IP

☐ 托管IP

选择关联机器

确定

取消

- 若您的 DDoS 高防包实例是共享包，**关联设备类型**与**选择关联机器**均允许多选，**选择关联机器**数量不得超过 [购买 DDoS 高防包实例](#) 时设置的IP 数量。

绑定设备

ID/服务包名

bgp-000000

地域

华南地区(广州)

可绑定IP数

5

已绑定设备

关联设备类型

☒ 云主机
 ☐ 负载均衡
 ☐ 黑石物理机
 ☐ 黑石负载均衡
 ☐ Web应用防火墙
 ☐ NAT网关
 ☐ VPN网关
 ☐ 弹性网卡
 ☐ GAAP
 ☐ 黑石弹性IP
 ☐ 托管IP

选择关联机器

输入主机 IP 或名称

☐
☒
☐
☐
☐
☐
☐
☐

已选择(2)

已选中机器2台(云主机1台,黑石弹性IP1台)

确定

取消

① 说明：

DDoS 高防包支持托管 IP，目前在白名单中。如用户使用腾讯云的托管 IP，需要接入 DDoS 高防包，请致电4009100100转1（工作日9:00am – 6:00pm）进行咨询，或 [提交工单](#) 申请加入白名单。

4. 单击确定。

版权所有：腾讯云计算（北京）有限责任公司

第104 共285页

操作指南

操作总览

最近更新时间：2023-07-21 09:44:35

您在使用 DDoS 高防包时，可能碰到诸如配置 DDoS 高防包实例、查看统计报表、查看操作日志以及设置安全事件通知等问题。本文将介绍使用 DDoS 高防包的常用操作，供您参考。

实例管理

- [查看实例详情](#)
- [设置资源名称](#)
- [配置弹性防护](#)
- [更换防护对象 IP](#)
- [解封防护 IP](#)

防护配置

- [配置清洗阈值与防护等级](#)
- [配置业务场景](#)
- [管理 DDoS 高级防护策略](#)
- [管理 CC 防护策略](#)

统计报表

[查看统计报表](#)

操作日志

[查看操作日志](#)

安全事件通知

[设置安全事件通知](#)

使用限制

最近更新时间：2023-07-21 09:44:35

防护对象限制

DDoS 高防包仅适用于腾讯云产品，包含云服务器、负载均衡、黑石物理服务器、NAT 网关等。

接入限制

DDoS 高防包仅支持绑定同一地域内的腾讯云公网 IP。

黑白名单配置限制

- DDoS 黑白 IP 名单之和最多支持添加100个 IP 地址。
- CC 黑白 IP 名单分别最多支持添加50个 IP 地址。
- CC URL 白名单最多支持添加50个 URL。

地域限制

DDoS 高防包只能绑定同一地域内的腾讯云设备，目前开放购买的地域包括：华北（北京）、华东（上海）、华南（广州）。DDoS 高防包在不同地域提供的高防能力请参考如下表格：

类型	地区	保底防护	弹性防护	最大防护能力
独享包	广州	5Gbps – 50Gbps	30Gbps – 100Gbps	100Gbps
	北京	5Gbps – 50Gbps	30Gbps – 100Gbps	100Gbps
	上海	5Gbps – 100Gbps	30Gbps – 300Gbps	300Gbps
共享包	广州	20Gbps 50Gbps 100Gbps	30Gbps – 100Gbps	100Gbps
	北京		30Gbps – 100Gbps	100Gbps
	上海		30Gbps – 300Gbps	300Gbps

实例管理

查看实例详情

最近更新时间：2023-07-21 09:44:36

操作场景

您可以通过 DDoS 防护管理控制台查看所购买的 DDoS 高防包的基础信息（如实例保底防护峰值、运行状态）及实例的弹性防护配置。

操作步骤

示例：查看广州地区独享包实例“bgp-000006ee”的详细信息。

1. 登录 [DDoS 防护管理控制台](#)，在左侧导航栏中，选择 **DDoS 高防包** > **资产列表**，单击**独享包**，在地区选择框中，单击**华南地区（广州）**，找到实例 ID 为“bgp-000006ee”的独享包，单击“ID/独享包名”查看实例信息。



2. 在弹出的页面中查看如下信息：

bgp-000006ee

基础信息

编辑

服务包名

所在地区

华南地区(广州)

绑定IP

保底防护峰值

20 Gbps

升级

当前状态

运行中

到期时间

2019-11-14 19:52:44

续费

标签

无

弹性防护

当前状态

未开启

开启

想要提升防御可开启弹性防护，无攻击不计费

参数分类	参数名称	说明
基础信息	服务包名	该 DDoS 高防包实例的名称，用于辨识与管理 DDoS 高防包实例。长度为1 – 20个字符，不限制字符类型。资源名称由用户根据实际业务需求自定义设置，具体操作请参考 设置资源名称 。
	所在地区	购买 DDoS 高防包时选择的地域。
	绑定 IP	该 DDoS 高防包实例所防护业务的实际 IP。
	保底防护峰值	该 DDoS 高防包实例的保底防护带宽能力，即购买时选择的保底防护峰值。 若未开启弹性防护，则保底防护峰值为高防服务实例的最高防护峰值。
	当前状态	DDoS 高防包实例当前的使用状态。状态包括运行中，清洗中以及封堵中等。
	到期时间	根据 购买 时选择的购买时长以及具体的提支付购买订单的具体时间计算所得，精确到秒级。腾讯云会在此时间前的前7天内，

弹性防护信息		通过站内信、短信及邮件的方式向腾讯云账号的创建者以及所有协作者推送服务即将到期并提醒及时续费的信息。
	标签	表示该 DDoS 高防包实例所属的标签名称，可以编辑、删除。
	当前状态	表示弹性防护是否开启。若购买 DDoS 高防包实例时未开启弹性防护，用户可在使用过程中自助开启，具体操作请参见 配置弹性防护 。
	弹性峰值	开启弹性防护时，该参数项才可见，表示当前 DDoS 高防包实例的最大弹性防护能力。用户可以根据自身业务需求，随时调整弹性防护峰值，具体操作请参见 配置弹性防护 。

设置资源名称

最近更新时间：2023-07-21 09:44:36

当使用多个 DDoS 高防包实例时，可通过设置**资源名称**快速辨识与管理实例。

方式一

1. 登录 [DDoS 防护管理控制台](#)，在左侧导航中，选择 **DDoS 高防包** > **资产列表**，在资产列表左上方，选择地域。
2. 单击目标实例的“ID/名称”列的名称，输入名称即可。

① 说明：

名称长度为1 - 20个字符，不限制字符类型。

ID/共享包名	所属地区
bgp-0000002a	华南地区(广州)
tengxunyuntest	

方式二

1. 登录 [DDoS 防护管理控制台](#)，在左侧导航中，选择 **DDoS 高防包** > **资产列表**，在资产列表左上方，选择地域。
2. 在下方实例列表中，单击目标实例的“ID/名称”列的实例名称，进入实例的基础信息页面。
3. 在实例的基础信息页面中，单击基础信息右侧的**编辑**，输入或修改名称，并单击**确定**即可。

基础信息	编辑
服务包名	
所在地区	华南地区(广州)
绑定IP	
保底防护峰值	20 Gbps
当前状态	运行中
到期时间	2020-01-06 15:49:36 续费
标签	无

① 说明：

名称长度为1 – 20个字符，不限制字符类型。

配置弹性防护

最近更新时间：2023-07-21 09:44:36

DDoS 高防包实例启用弹性防护后，当攻击流量峰值超出保底防护峰值时，DDoS 高防包会根据用户设置的弹性防护峰值继续进行防护。

若 [购买 DDoS 高防包实例](#) 时，未开启弹性防护，用户可在使用过程中自助开启。当天未触发弹性防护，不产生额外费用。在触发弹性防护（攻击峰值超过保底防护峰值）时，取当天实际产生的最高攻击峰值所对应区间进行 [计费](#)，账单次日生成。用户可根据实际业务情况实时更改 DDoS 高防包实例的弹性防护峰值。

开启弹性防护

说明：

若 [购买 DDoS 高防包实例](#) 时未开启弹性防护，用户可在使用过程中开启，并以历史最高攻击流量为参考，选择略高于历史最高峰值的弹性防护峰值，以便足够防御大流量攻击，避免超过防护峰值而引起的 IP 封堵。

1. 登录 [DDoS 防护管理控制台](#)，选择 **DDoS 高防包** > **资产列表**，在目标实例所在行，单击**开启弹性防护**。
2. 在**开启弹性防护**对话框中，选择合适的**弹性防护峰值**。

开启弹性防护

ID/服务包名

bgp-

当前带宽峰值

30Gbps

弹性防护峰值

40Gbps

50Gbps

60Gbps

70Gbps

80Gbps

90Gbps

100Gbps

120Gbps

150Gbps

200Gbps

250Gbps

300Gbps

在带宽峰值30Gbps的基础上，最高能够防御40Gbps的DDoS的攻击

费用说明

未触发弹性防护，不另收费用。

如果攻击发生当日流量带宽峰值超出30Gbps，会按照当日流量带宽峰值落入的计费区间进行计算，产生后付费账单。

计费区间如下：

弹性防护峰值(Gbps)	20~30	30~40	40~50	50~60	60~70	70~80	80~90	90~100	100~120	120~150	150~200	200~250	250~300
弹性防护费用(元/天)	3500	4800	5700	6600	7500	8350	9200	10050	11750	14300	18550	22800	26800

确定提交

取消

3. 单击**确定提交**。

更改弹性防护峰值

1. 登录 [DDoS 防护管理控制台](#)，选择 **DDoS 高防包** > **资产列表**，单击目的实例，进入实例的基础信息界面。

2. 找到“弹性防护”部分，单击**防护峰值**右侧的**更改**。

服务包信息 [编辑](#)

服务包名

所在地区

华南地区(广州)

绑定IP

保底防护峰值

20 Gbps

[升级](#)

当前状态

运行中

到期时间

2019-04-18 18:24:51

[续费](#)

弹性防护

当前状态

已开启

[关闭](#)

防护峰值

50Gbps

[更改](#)

3. 在**更改弹性防护**对话框中，选择合适的**弹性防护峰值**。

① 说明：

- 弹性防护峰值支持调升调降，不同地域支持的防护能力不同，弹性防护峰值的具体取值范围请参考 [使用限制](#)。
- 弹性防护峰值修改后立即生效。

更改弹性防护

ID/服务包名

当前带宽峰值

30Gbps

弹性防护峰值

40Gbps

50Gbps

60Gbps

70Gbps

80Gbps

90Gbps

100Gbps

120Gbps

150Gbps

200Gbps

250Gbps

300Gbps

在带宽峰值30Gbps的基础上，最高能够防御40Gbps的DDoS的攻击

费用说明

未触发弹性防护，不另收费用。
如果攻击发生当日流量带宽峰值超出30Gbps，会按照当日流量带宽峰值落入的计费区间进行计算，产生后付费账单。
计费区间如下：

弹性防护峰值(Gbps)	20~30	30~40	40~50	50~60	60~70	70~80	80~90	90~100	100~120	120~150	150~200	200~250	250~300
弹性防护费用(元/天)	3500	4800	5700	6600	7500	8350	9200	10050	11750	14300	18550	22800	26800

确定提交

取消

4. 单击**确定提交**。

关闭弹性防护

① 说明：

关闭弹性防护后，最大防护峰值降为保底防护峰值，请确保是否满足实际需求再执行此操作。

1. 登录 [DDoS 防护管理控制台](#)，选择 **DDoS 高防包 > 资产列表**，在目标实例所在行，单击**关闭弹性防护**。
2. 在**关闭弹性防护**对话框中，单击**确定提交**。

管理防护对象 IP

最近更新时间：2023-07-21 09:44:36

操作场景

DDoS 高防包为腾讯云公网 IP 提供更高的 DDoS 防护能力，可支持防护 CVM、CLB、NAT、WAF 等产品和服务。

用户根据实际业务需求，可以更换已绑定到 DDoS 高防包实例的防护对象 IP，也可以一键解绑已绑定到 DDoS 高防包的防护对象 IP。

前提条件

在更换、或解绑防护对象 IP，您需要成功 [购买 DDoS 高防包实例](#) 并已为其 [绑定防护对象 IP](#)。

操作步骤

更换防护对象 IP

1. 登录 [DDoS 防护管理控制台](#)，在左侧导航中，选择 **DDoS 高防包** > **资产列表**，在页面上方，选择地域。
 - 若您的 DDoS 高防包实例是独享包，则选择**独享包**页签。
 - 若您的 DDoS 高防包实例是共享包，则选择**共享包**页签。
2. 单击目标 DDoS 高防包实例所在行的**更换设备**。
3. 在**绑定设备**页面，根据实际防护需求选择**关联设备类型**与**选择关联机器**。
 - 若您的 DDoS 高防包实例是独享包，仅支持绑定一个关联机器。

绑定设备

ID/服务包名

bgp-000005vg

地域

华东地区(上海)

已绑定设备

212.64.27.149

关联设备类型

☒ 云主机

☐ 负载均衡

☐ 黑石物理机

☐ 黑石负载均衡

☐ Web应用防火墙

☐ NAT网关

☐ VPN网关

☐ 弹性网卡

☐ GAAP

☐ 黑石弹性IP

☐ 托管IP

选择关联机器

输入主机 IP 或名称

- 若您的 DDoS 高防包实例是共享包，关联设备类型与选择关联机器均允许多选，选择关联机器数量不得超过 [购买 DDoS 高防包实例](#) 时设置的IP 数量。

绑定设备

ID/服务包名

bgp-0000003

地域

华东地区(上海)

可绑定IP数

5

已绑定设备

关联设备类型

☒ 云主机

☐ 负载均衡

☐ 黑石物理机

☐ 黑石负载均衡

☐ Web应用防火墙

☐ NAT网关

☐ VPN网关

☐ 弹性网卡

☐ GAAP

☐ 黑石弹性IP

☐ 托管IP

选择关联机器

输入主机 IP 或名称

☐

☒

已选择(2)

4. 单击确定。

解绑防护对象 IP

1. 登录 [DDoS 防护管理控制台](#)，在左侧导航中，选择 **DDoS 高防包** > **资产列表**，在页面上方，选择地域。
 - 若您的 DDoS 高防包实例是独享包，则选择**独享包**页签。
 - 若您的 DDoS 高防包实例是共享包，则选择**共享包**页签。
2. 单击目标 DDoS 高防包实例所在行的**更多**>**解绑**，在弹出的会话框中，单击**确定**即可。



解封防护 IP

最近更新时间：2023-07-27 11:17:12

DDoS 高防包对进入封堵状态的防护 IP 提供解封的功能，您可以登录 [DDoS 防护管理控制台](#) 进行自助解封操作。

自助解封次数

使用 DDoS 高防包的用户每天将拥有三次自助解封机会，当天超过三次后将无法进行解封操作。系统将在每天零点时重置自助解封次数，当天未使用的解封次数不会累计到次日。

说明：

- 由于解封涉及腾讯云 DDoS 防护系统的风控管理策略，解封可能失败（解封失败不会扣减您的剩余解封次数），请您耐心等待一段时间后再次尝试。
- 在执行解封操作前，建议您先查看预计解封时间，预计解封时间受到部分因素影响，可能会推后。如果您可以接受预计时间，则无需手动操作。
- 当天自助解封配额为0时，建议提升保底防护能力或弹性防护能力，以便足够防御大流量攻击，避免被持续封堵。

自助解封操作

登录 [DDoS 防护管理控制台](#)，选择自助解封 > 解封操作，找到状态为自动解封中的防护 IP，单击操作列中的解封。在解除封堵对话框中，单击确定。

- 如果解封失败，您会收到解封失败提示信息，请您耐心等待一段时间后再尝试。
- 如果收到解封成功提示信息，则表示封堵状态已成功解除，您可以刷新页面确认该防护 IP 是否已恢复运行中状态。

解封操作				
总配额数		当前已使用		当前未使用
3 次		0 次		3 次
IP	封堵时间	预计解封时间	状态	操作
119.29.245.153	2018-11-07 20:31:37	2018-11-07 22:31:37	自动解封中	解封

解封操作记录

登录 [DDoS 防护管理控制台](#)，选择自助解封 > 解封操作记录，根据时间范围筛选，可查看所有解封操作记录，包括自动解封、手工自助解封等操作记录。

解封操作记录

2018-08-09 20:38:41 至 2018-11-07 20:38:41 

IP	封堵时间	实际解封时间	解封操作类型
123.206. 	2018-10-18 15:49:52	2018-10-18 16:05:09	自助解封
123.206. 	2018-10-17 16:21:40	2018-10-17 16:52:02	自动解封
123.206. 	2018-10-17 16:16:50	2018-10-17 16:47:16	自动解封
193.112. 	2018-09-14 17:37:45	2018-09-14 18:17:26	自助解封

防护配置

配置清洗阈值与防护等级

最近更新时间：2023-07-21 09:44:36

应用场景

DDoS 高防包服务提供防护策略调整功能，针对 DDoS 攻击提供三种防护等级供您选择，各个防护等级的具体防护操作如下：

防护等级	防护操作	描述
宽松	- 过滤明确攻击特征的 SYN、ACK 数据包。 - 过滤不符合协议规范的 TCP、UDP、ICMP 数据包。 - 过滤具有明确攻击特征的 UDP 数据包。	- 清洗策略相对宽松，仅对具有明确攻击特征的攻击包进行防护。 - 建议在怀疑有误杀时启用，遇到复杂攻击时可能会有攻击透传。
正常	- 过滤明确攻击特征的 SYN、ACK 数据包。 - 过滤不符合协议规范的 TCP、UDP、ICMP 数据包。 - 过滤具有明确攻击特征的 UDP 数据包。 - 过滤常见基于 UDP 的攻击数据包。 - 对部分访问源 IP 进行主动验证。	- 清洗策略适配绝大多数业务，可有效防护常见攻击。 - 默认为正常模式。
严格	- 过滤明确攻击特征的 SYN、ACK 数据包。 - 过滤不符合协议规范的 TCP、UDP、ICMP 数据包。 - 过滤具有明确攻击特征的 UDP 数据包。 - 过滤常见基于 UDP 的攻击数据包。 - 对部分访问源 IP 进行主动验证。 - 过滤 ICMP 攻击包。 - 过滤常见的 UDP 攻击数据包。	清洗策略相对严格，建议在正常模式出现攻击透传时使用。

- UDP 数据包严格检查。

① 说明：

如果您的业务需要使用 UDP，建议您联系 [腾讯云技术支持](#) 进行策略定制，以免严格模式影响业务流程。

默认情况下，您所购买的 DDoS 高防包实例采用正常防护等级，您可以根据实际业务情况自由调整 DDoS 防护等级。同时，您还可以自定义设置清洗阈值，当攻击流量超过设置的阈值时，将启动清洗。

配置示例

下面以配置华南地区（广州）的实例“bgp-000006ee”为例，进行配置说明：

1. 登录 [DDoS 防护管理控制台](#)，在左侧导航栏中，选择 **DDoS 高防包** > **资产列表**，单击**独享包**，在地区选择框中，单击**华南地区（广州）**，找到实例 ID 为“bgp-000006ee”的独享包，在右侧操作项中，单击**防护配置**进行配置。
2. 在弹出的 DDoS 防护配置的页面中，开启**防护状态**，进行清洗阈值、防护等级的设置。

DDoS防护配置

防护状态	☒
清洗阈值 ①	默认 ▼
防护等级 ①	宽松 正常 严格
业务场景	无 ▼
高级策略	无 ▼
DDoS攻击告警阈值	未设置 ▼
TCP业务AI增强防护	☐

① 说明：

仅当“防护状态”为 ☒ 状态时，下面配置项才可见。若手动将防护状态关闭，则配置项隐藏且配置不生效，重新开启后，配置项可见且保持原有的配置数据。

配置参数说明：

● 防护状态

默认开启，您可根据实际业务需求开启或关闭防护。关闭防护时，可进行关闭时长的设置，目前只能临时关闭防护1 - 6小时，超过所设置的时长或当攻击流量超过100wpps或2Gbps时，DDoS 高防包将自动开启防护。

● 清洗阈值

- 清洗阈值是高防产品启动清洗动作的阈值。当流量小于阈值时，即使检测到攻击也不会进行清洗操作。
- 默认在开启“防护状态”的情况下，业务刚接入的 DDoS 高防包实例的清洗阈值采用默认值，并随着接入业务流量的变化规律，系统自动学习形成一个基线值。您可以根据实际业务情况自由设置清洗阈值。

① 说明：

若明确该清洗阈值，可进行自定义设置。若无法明确该清洗阈值，DDoS 防护系统将根据 AI 算法自动学习并生成一套专属的默认阈值。

● 防护等级

默认在开启“防护状态”的情况下，业务刚接入的 DDoS 高防包实例采用正常防护等级，您可以根据实际业务防护需求自由调整 DDoS 防护等级。

● 其他配置项

○ 业务场景

您可以根据实际业务需求，从已创建的业务场景中选择一个匹配的业务场景，支持修改。当选择某一个业务场景后，对应的“高级策略”会自动匹配该业务场景生成的策略。请参见 [配置业务场景](#) 进行业务场景创建。

○ 高级策略

您可根据业务防护特性，从已创建的高级策略中选择一个匹配的高级策略，支持修改。请参见 [管理 DDoS 高级防护策略](#) 进行高级防护策略创建。

○ DDoS 攻击告警阈值

新增 DDoS 攻击告警阈值配置功能。若检测的指标超过您设定的阈值，将触发告警，并向您推送攻击告警信息。请参见 [配置攻击告警阈值](#) 进行告警指标设置。

○ TCP 业务 AI 增强防护

针对四层 TCP 业务，DDoS 高防包提供 TCP 业务 AI 增强防护功能，开启后，通过 AI 模型日常业务特征的自学习，能够自动识别业务流量与攻击流量，有效防护线上的四层 CC 攻击。

① 说明：

目前 TCP 业务 AI 增强防护功能仅对白名单开放。

配置业务场景

最近更新时间：2023-07-21 09:44:36

应用场景

DDoS 高防包支持自定义 DDoS 高级防护策略，用户可以根据业务特点或攻击行为针对性地设置防护策略。通常每个高防包实例最多绑定一个 DDoS 高级防护策略。当用户的账号下拥有多个高防包实例时，最多拥有5个 DDoS 高级防护策略可供选择。

为满足实际业务需要或应对不断变化的攻击手法，用户可能需要不断优化策略配置。为简化 DDoS 精细化防护管理，DDoS 高防包提供业务场景设置功能，通过创建业务应用场景，后台收集、识别并自动生成高级防护策略，实现灵活的配置或维护策略。

创建业务场景

方法一

若用户所购 DDoS 高防包实例未配置业务场景，登录 [DDoS 防护管理控制台](#)，在左侧导航中选择**DDoS 高防包 > 防护配置**，会弹出如下图所示的提示信息，单击**去创建**，进行业务场景的创建。



① 说明：

最多支持创建5个业务场景。

方法二

1. 登录 [DDoS 防护管理控制台](#)，在左侧导航中选择 **BGP 高防包 > 防护配置**，在防护配置页面中，选择 **DDoS 高级防护策略 > 创建业务场景**。

防护配置

独享包

防护策略

CC攻击防护

DDoS高级防护策略

创建业务场景

业务名称

高级策略名称

2. 在创建业务场景页面，根据实际业务特点，输入以下参数，单击确定完成1个业务场景的设置。

创建业务场景

业务名称(必填)

平台开发

☐ PC客户端
 ☐ 移动端
 ☐ 电视端
 ☐ 主机

细分品类

无

基础信息

当前正在使用的协议

☒ TCP协议
 ☒ UDP协议
 ☐ ICMP协议
 ☐ 其他协议

TCP业务端口范围?

-

UDP业务端口范围?

-

是否有海外客户?

☐ 是
 ☐ 否

是否会主动对外发起TCP请求?

☐ 是
 ☐ 否

是否会主动向外发起UDP业务请求(如DNS请求, NTP请求等)?

☐ 是
 ☐ 否

其他信息 收起

UDP载荷是否有固定特征?

☐ 是
 ☒ 否

TCP载荷是否存在固定特征?

☐ 是
 ☒ 否

是否存在Web API业务? (使用,分隔)

☐ 是
 ☒ 否

是否存在VPN业务?

☐ 是
 ☒ 否

TCP业务报文包长范围?

-

UDP业务报文包长范围?

-

确定

取消

- **业务名称**：必填项，输入业务名称，长度为1 – 32个字符，不限制字符类型。
- **平台开发**：勾选平台开发对应的类型。可供选择的有 PC 客户端、移动端、电视端和主机。
- **细分品类**：选择业务所属类型。可供选择的有游戏、应用、网站或其他类型。

- 基础信息：

- 当前正在使用的协议：勾选正在使用的协议，支持可选的协议有 ICMP、TCP、UDP 和其他协议（指除了 ICMP、TCP、UDP 以外的协议）。

① 说明：

当勾选 TCP、UDP 协议时，则需要输入 TCP/UDP 业务端口范围，可填范围为 1 - 65535，同时其他信息区域会弹出 TCP/UDP 业务报文包长范围配置，该配置为选填项，可填的报文包长范围为 0 - 1500。

- 是否有海外客户？

勾选是或否，对应生成策略的配置项为关闭 / 开启拒绝海外流量。

- 是否会主动对外发起 TCP 请求？

勾选是或否。选择是，需要填写主动对外发起 TCP 请求的端口。存在多个请求业务端口时，全部填入并用英文“,”分隔。

- 是否会主动向外发起 UDP 业务请求（DNS 请求，NTP 请求等）？

勾选是或否。选择是，需要填写主动对外发起 UDP 业务请求的端口。存在多个请求业务端口时，全部填入并用英文“,”分隔。

- 其他信息：（单击**展开+**即可选择对应参数）

- UDP 载荷是否有固定特征？

勾选是或否。默认否，当选择是时，需要填写 UDP 载荷特征内容。

- TCP 载荷是否存在固定特征？

勾选是或否。默认否，当选择是时，需要填写 TCP 载荷特征内容。

- 是否存在 Web API 业务？

勾选是或否。默认否，当选择是时，需要填写 API 业务 URL。存在多个 API 业务 URL 时，全部填入并用英文“,”分隔。

- 是否存在 VPN 业务？

勾选是或否。默认否，若选择是时，则不会禁用“其他协议”。

① 说明：

在“当前正在使用的协议”、“是否存在 VPN 业务”两项参数中，只要存在条件之一即勾选“其他协议”或选择“是存在 VPN 业务”，则不会禁用“其他协议”。

3. 后台对用户创建的业务场景进行分析后，自动生成1条以“业务场景名称_policy_序

号”（如“test_policy_1”）命名的高级防护策略，用户再根据实际特殊业务防护需求，自主配置或调整该条防护策略。

① 注意：

- 在用户只拥有一个 DDoS 高防包实例的情况下，若只创建一个业务场景，则自动将对应生成的高级防护策略绑定到当前实例中。

- 当对业务场景信息修改后，对应生成的高级防护策略会自动同步相关配置项信息。若对该条高级防护策略进行调整，则不会同步到对应的业务场景信息。

修改和删除业务场景

- 登录 [DDoS 防护管理控制台](#)，在左侧导航中选择 **DDoS 高防包** > **防护配置**。
- 在 **DDoS 高级防护策略** 页面，找到目的业务场景，单击 **配置** 或 **删除**，进行修改或者删除。

① 说明：

当对目的业务场景进行删除操作，则对应的高级防护策略也将删除。

创建业务场景			
业务名称	高级策略名称	创建时间	操作
test	test_policy_82	2019-07-01 19:42:12	配置 删除

若需要了解更多信息，请参见 [管理 DDoS 高级防护策略](#)。

管理 DDoS 高级防护策略

最近更新时间：2024-12-06 17:36:32

DDoS 高防包提供面向 DDoS 攻击的高级防护策略功能，用户可针对自身业务防护需求对 DDoS 防护策略进行调整和优化。通过黑白名单、禁用协议、禁用端口、报文特征过滤策略、连接耗尽防护、水印防护等功能，为业务提供针对性防护。

配置项简介

配置项	功能简介	生效时间
黑白名单	基于 IP 地址级别的防护。 - 白名单中的 IP，访问时将被直接放行，不经过任何防护策略过滤。 - 黑名单中的 IP，访问时将会被直接阻断。	当被防护的 IP 处于被攻击状态时生效。
禁用协议	可禁用业务不使用的协议。 当检测到攻击行为时，DDoS 高防集群会清洗掉该协议的流量。	当被防护的 IP 处于被攻击状态时生效。
禁用端口	可禁用业务不使用的端口。 当检测到攻击行为时，DDoS 高防集群会清洗掉该端口的流量。	当被防护的 IP 处于被攻击状态时生效。
报文过滤特征	可以针对业务报文特征或攻击报文特征，将协议、端口范围、包长范围、是否检测载荷、偏移量、检查深度、是否包括特征字符串等条件进行组合，设定策略动作。当检测到报文匹配到策略条件时，可以执行直接转发、丢弃、拉黑源 IP 或断开连接等操作。	当被防护的 IP 处于被攻击状态时生效。
限速	基于目的 IP 的防护，对访问协议进行限速控制。	当被防护的 IP 处于被攻击状态时生效。
拒绝海外流量	可拒绝来自中国（大陆地区及港澳台）以外的 TCP 流量请求。	当被防护的 IP 处于被攻击状态时生效。
空连接防护	应对空连接攻击。	当被防护的 IP 处于被攻击状态时生效。
连接耗尽防护	基于 IP 地址的防护，对于接入高防包的防护 IP 的连接速度、包长度等参数进行限制，实现缓解小流量的连接型攻击的防护功能。	当被防护的 IP 处于被攻击状态时生效。

异常连接检测	当一个源 IP 接收到的一个 TCP 连接符合所配置的参数特征时，将判断为异常连接，同时当该源 IP 所接收到的异常连接数超过所设置的最大异常连接数时，会被加入黑名单一定时间，禁止被访问。	当被防护的 IP 处于被攻击状态时生效。
水印防护	支持 UDP 和 TCP 报文，在配置的端口范围内，其载荷进行水印检测和剥离。通过接入水印防护，高效全面防护 4 层 CC 攻击，如模拟业务报文攻击和重放攻击等。 - 业务端和腾讯云 DDoS 安全防护系统端共享水印算法和密钥。 - 客户端每个发出的报文都嵌入了水印特征，而攻击报文却无水印特征。 - DDoS 安全防护系统将甄别出攻击报文并将其丢弃。	当被防护的 IP 处于被攻击状态时生效。

添加新策略

① 注意：

高级安全防护策略功能具有一定专业性，建议有相关经验的用户在阅读以下操作指南后根据实际情况进行配置。

登录 [DDoS 防护管理控制台](#)，选择 **DDoS 高防包 > 防护配置**。在 **DDoS 高级防护策略**页签，单击**添加新策略**。根据实际业务需求设置以下参数，单击**确定**。

策略名称

黑白名单

添加

请输入要查询的IP

策略	地址	操作
记录为空		

共0项

每页显示行 10

高级安全策略

禁用协议

☐ ICMP ☐ TCP ☐ UDP ☐ 其他协议

禁用端口

协议	开始端口号	结束端口号	操作
暂无记录，点击添加			

报文过滤特征

协议	开始源端	结束源端	开始目的	结束目的	最小包长	最大包长	检测载荷	正则表达	偏移量	检查深度	是否包括	字符串	策略	操作
暂无记录，点击添加														

限速

协议	限速阈值	操作
暂无记录，点击添加		

拒绝海外流量

拒绝海外流量 ☒ 关闭 ☐ 开启

策略名称

输入策略名称，长度为1 – 32个字符，不限制字符类型。

黑白名单

- 若需设置黑名单：单击添加，选择黑名单，填写需要拦截的 IP，存在多个 IP 时可全部填入并用回车分隔多个 IP，单击确定。
- 若需设置白名单：单击添加，选择白名单，填写需要放行的 IP，存在多个 IP 时可全部填入并用回车分隔多个 IP，单击确定。

说明：

黑白 IP 名单之和最多支持添加100个 IP，批量添加的 IP 数不允许超过当前配额。



● 禁用协议

选择需要禁用的协议。

● 禁用端口

选择协议和端口类型，然后填写对应需要禁用的端口。若某条记录中仅需禁用一个端口，则开始端口号和结束端口号填写相同值即可。单击列表下方的**增加**可新增多条记录。协议包括TCP、UDP两种协议，端口类型包括目的端口、源端口、目的端口和源端口三种类型。

● 报文过滤特征

支持将协议、端口范围、包长范围、是否检测载荷、偏移量、检查深度、是否包括特征字符串等条件进行组合，设定策略动作且即刻生效。

① 说明：

- 偏移量：表示报文内容中开始匹配的特征的位置。
- 检查深度：配合偏移量使用，表示从偏移量设定的位置开始向后匹配的报文内容长度。
- 策略：
 - “丢弃报文”表示丢弃匹配该报文过滤特征的数据包。
 - “丢弃且拉黑源 IP”表示丢弃匹配该报文过滤特征的数据包并将源 IP 临时拉黑一段时间。
 - “丢弃且断开连接”表示丢弃匹配该报文过滤特征的数据包并断开 TCP 连接。
 - “丢弃，断开连接且拉黑源 IP”表示丢弃匹配该报文过滤特征的数据包，同时断开 TCP 连接并将源 IP 临时拉黑一段时间。
 - “直接转发”表示直接转发匹配该报文过滤特征的数据包。

● 限速

单击**添加**，选择需要限速的协议，设置限速阈值。支持限速的可选协议有 ICMP、TCP、UDP 和其他协议，这里的其他协议指除了 ICMP、TCP、UDP 以外的协议。

● 拒绝海外流量

勾选开启或关闭。DDoS 高防包的防护引擎内置海外 IP 库，开启拒绝海外流量后将基于该 IP 库对来源进行判断并执行阻断。勾选**开启**时，需处于被攻击状态才生效。勾选**关闭**时即刻生效。

连接耗尽防护

空连接防护 ①

☒ 关闭 ☐ 开启

源新建连接限速

☒ 关闭 ☐ 开启

源并发连接限制

☒ 关闭 ☐ 开启

目的新建连接限速

☒ 关闭 ☐ 开启

目的并发连接数限制

☒ 关闭 ☐ 开启

异常连接检测 ①

☒ 关闭 ☐ 开启

源IP最大异常连接数

☒ 关闭 ☐ 开启

水印防护

TCP防护端口	UDP防护端口	UDP水印剥离	策略开关	操作
点击开启				

确定

取消

● 连接耗尽防护

- **空连接防护**：勾选开启或关闭。勾选开启时，需处于被攻击状态才生效。由于基于 TCP 代理原理实现，对于业务的首次访问体验可能会有影响。
- **源新建连接限速**：勾选开启或关闭。勾选开启时，设置抑制速率（单位：个/秒），可填范围 0-∞。表示单一源IP每秒新建连接速率，超过限制的新建连接将被丢弃。
- **源并发连接限速**：勾选开启或关闭。勾选开启时，设置抑制数（单位：个），可填范围 0-∞。表示单一源IP并发连接数，超过限制的并发连接将被丢弃。
- **目的新建连接限速**：勾选开启或关闭。勾选开启时，设置抑制速率（单位：个/秒），可填范围 0-∞。表示目的IP每秒最大新建连接速率，超过限制的新建连接将被丢弃。由于防护设备为集群化部署，新建连接限速存在一定误差。
- **目的并发连接限速**：勾选开启或关闭。勾选开启时，设置抑制数（单位：个），可填范围 0-∞。表示目的IP 最大并发连接数，超过限制的并发连接将被丢弃。由于防护设备为集群化部署，并发连接限速存在一定误差。

● 异常连接检测

- **源 IP 最大异常连接数**：单击开启，填写源 IP 最大异常连接数量，可填范围 0-∞（单位：个）。表示当一个源 IP 符合异常连接行为识别的连接数，超过所指定阈值时，会被认为是异常攻击源，在一定时间内被限制访问。

① 说明：

只有开启源 IP 最大异常连接数，以下参数才能进行配置。

- **Syn 报文占比检测**：勾选开启或关闭。勾选开启时，设置 Syn 报文占比值，可填范围 0-100。表示当一个 TCP 连接中的 Syn 报文数与 Ack 报文数的比例超过所配置阈值时，会被识别为一个异常连接。
- **Syn 报文数检测**：勾选开启或关闭。勾选开启时，设置最大报文数，可填范围 0-65535。表示当一个 TCP 连接中的 Syn 报文数超过所配置最大报文数时，会被识别为异常连接。

- **连接超时检测**：勾选开启或关闭。勾选**开启**时，设置检测周期（单位：秒），可填范围 0-65535。表示一个 TCP 连接创建后在所设置的时间内没有任何报文传输则判断为异常连接。
- **异常空连接检测**：勾选开启或关闭。表示一个 TCP 连接创建后没有任何带有载荷的报文传输则判断为异常连接。

- **水印防护**

单击**开启**进行水印防护配置。填写指定的 TCP 协议防护端口和 UDP 协议防护端口，单击**确定**水印防护功能即刻开启。添加 DDoS 高级防护策略后，自动产生一条密钥信息，需要完成线下客户端接入水印配置。

水印创建

TCP协议防护端口

开始端口号	结束端口号	操作
暂无记录，点击 添加		

TCP防护端口最多可以配置5个端口段；不同端口段不可以互相重合；起止端口号相同则认为是一个端口；TCP或UDP协议端口段需要至少配置一条。

UDP协议防护端口

开始端口号	结束端口号	操作
暂无记录，点击 添加		

UDP防护端口最多可以配置5个端口段；不同端口段不可以互相重合；起止端口号相同则认为是一个端口；TCP或UDP协议端口段需要至少配置一条。

确定

取消

- **TCP 协议防护端口、UDP 协议防护端口**

TCP/UDP 防护端口最多可以配置5个端口段；不同端口段不可以互相重合；起止端口号相同则认为是一个端口；TCP 或 UDP 协议端口段中需要至少配置一条。

绑定与解绑资源

登录 [DDoS 防护管理控制台](#)，选择DDoS 高防包 > 防护配置。在 DDoS 高级防护策略页签，单击目标策略所在行的**绑定资源**。

- **绑定资源**：在弹出的**绑定资源**对话框中，根据实际业务需求勾选一个或多个资源，单击**确定**。
- **解绑资源**：在弹出的**绑定资源**对话框中，根据实际业务需求单击**已选择**区域中已选资源右侧的 ，单击**确定**。

添加新策略			
策略名称	绑定资源数量	创建时间	操作
	0	2019-04-15 09:41:40	配置 删除 绑定资源 水印密钥配置 水印客户端接入文件下载
	0	2019-04-15 15:18:32	配置 删除 绑定资源 水印密钥配置 水印客户端接入文件下载

客户端接入水印

登录 [DDoS 防护管理控制台](#)，选择 **DDoS 高防包 > 防护配置**。在 **DDoS 高级防护策略** 页签，单击目标策略所在行的 **水印客户端文件下载**，线下完成客户端的接入。

添加、删除或停用/启用水印密钥

登录 [DDoS 防护管理控制台](#)，选择 **DDoS 高防包 > 防护配置**。在 **DDoS 高级防护策略** 页签，单击目标策略所在行的 **水印密钥配置**。

- **添加密钥**：在弹出的**密钥信息**对话框中，单击**添加密钥**即刻生成新密钥。
- **停用/启用密钥**：支持对密钥进行停用或启用操作。在弹出的**密钥信息**对话框中，单击目的密钥所在行的**停用**；如需重新开启则单击**启用**即可。
- **删除密钥**：只能对已停用的密钥进行删除。在弹出的**密钥信息**对话框中，单击目的密钥所在行的**删除**即可。

① 说明：

最多可存在2个密钥，如果需要添加新密钥，请先删掉其中一个旧密钥；当仅有一个密钥生效时，不可将其停用或删除。

密钥信息

每个业务最多可以使用2个密钥，如果您需要添加新密钥，请先删除旧密钥；当仅有一个生效密钥时，不可停用和删除。

密钥	状态	生成时间	操作
	已停用	2019-04-18 18:57:45	复制 启用 删除
	已开启	2019-04-22 17:04:13	复制 停用

[添加密钥](#)[取消](#)

配置策略

登录 [DDoS 防护管理控制台](#)，选择 **DDoS 高防包 > 防护配置**。在 **DDoS 高级防护策略** 页签，单击目标策略所在行的 **配置**。根据实际业务需求更新以下参数，单击**确定**保存修改。

① 说明：

当目的策略是以“业务场景名称_policy_序号”形式命名的，则不能对策略名称进行修改。

- 策略名称
- 黑白名单
- 禁用协议
- 禁用端口
- 报文过滤特征
- 拒绝海外流量
- 连接耗尽防护
- 异常连接检测
- 水印防护

删除策略

① 说明：

- 未绑定资源的策略可直接删除，已绑定资源的策略需要先将所有资源解绑再执行删除操作；策略删除后不可恢复，请谨慎操作。
- 不能对根据用户创建的业务场景自动生成的高级防护策略进行删除操作。

登录 [DDoS 防护管理控制台](#)，选择 **DDoS 高防包 > 防护配置**。在 **DDoS 高级防护策略**页签，单击目标策略所在行的**删除**。在弹出的对话框中，单击**确定**。

删除高级策略



确认删除该策略吗？

删除策略后，该防护策略将从列表中永久删除，不可恢复。
确定删除该条高级策略

确定

取消

配置 CC 防护策略

最近更新时间：2023-07-21 09:44:37

操作场景

DDoS 高防包支持 CC 防护功能，当高防包统计的 HTTP 请求量超过设定的 **http 请求数阈值**时，自动触发 CC 防护。同时，DDoS 高防包还支持 URL 白名单、IP 白名单和 IP 黑名单策略：

- 白名单中的 URL，其访问请求将无需执行 CC 攻击检测，直接被放行。
- 白名单中 IP，其 HTTP 访问请求将无需执行 CC 攻击检测，直接被放行。
- 黑名单中 IP，其 HTTP 访问请求将直接被拒绝。

用户可根据业务特点和防护需求，自定义防护策略实现更精准的 CC 攻击拦截。

操作步骤

1. 登录 [DDoS 防护管理控制台](#)，选择 **DDoS 高防包 > 防护配置**，在 **CC 防护**页签，选择目标地域和高防包实例，进行 CC 防护配置。

CC防护

☒ 对于敏感业务，可将业务URL添加到URL白名单，对该业务不做CC攻击检测和防护

http请求数阈值

1500 QPS

当http请求数超过设定值时，触发CC防护。

添加策略

最多可以添加5条策略

请输入要查找的策略名称

策略名称	匹配条件	匹配动作	创建时间	当前状态	操作
test	1-100	拦截	2019-05-21 17:03:42	☒	编辑 删除
test	1-100	拦截	2019-05-21 17:03:23	☒	编辑 删除

共2项

每页显示 10 1/1

URL白名单

IP白名单

IP黑名单

添加 URL

删除

最多可以添加50条URL

☐ URL

操作

2. 单击**CC 防护**右侧的  开启 CC 防护。

说明：

- CC 防护默认关闭。

- 开启 CC 防护后，才可设置 HTTP 请求数阈值、自定义 CC 防护策略以及黑白名单。

3. 单击 **http 请求数阈值** 右侧的下拉框选择合适的阈值。

4. 单击 **添加访问控制策略**，在 **添加访问控制策略** 弹出框中，根据实际业务需求设置以下参数，单击 **确定** 完成配置。

添加访问控制策略

×

请添加需要访问控制策略，添加完成后默认开启该策略

策略名称

请输入策略名称，最长20个字

模式

☒ 匹配模式 ☐ 限速模式

策略

当

host

包含

时

+添加一行

执行

拦截

确定

取消

① 说明：

- 仅在该高防包正在被攻击状态时，自定义策略才会生效。
- 匹配模式下，每个自定义策略最多可以设置4个策略条件进行特征控制，且多个条件之间是“与”的关系，需要所有条件全部匹配策略才生效。
- 限速模式下，每个自定义策略只允许设置1条策略条件。

• 策略名称

输入策略名称，长度为1 – 20字符，不限制字符类型。

• 模式

- 匹配模式：匹配到 HTTP 对应字段头的请求，执行拦截或人机识别操作。
- 限速模式：对源 IP 访问进行限速处理。

○ 策略

- 当选择**匹配模式**时，支持从 HTTP 报文的 host 参数、CGI 参数、Referer 和 User-Agent 等多个特征进行组合，组合逻辑包括包含、不包含和等于。最多可以设置4个策略条件进行特征控制，字段描述如下：

匹配字段	字段描述	适用的逻辑符
host	访问请求的域名。	包含、不包含、等于。
CGI	访问请求的 URL 地址。	包含、不包含、等于。
Referer	访问请求的来源网址，表示该访问请求是从哪个页面跳转产生的。	包含、不包含、等于。
User-Agent	发起访问请求的客户端浏览器标识等相关信息。	包含、不包含、等于。

- 当选择**限速模式**时，对每个源 IP 访问进行限速处理。只允许设置1个策略条件。

添加访问控制策略

×

请添加需要访问控制策略，添加完成后默认开启该策略

策略名称

模式

☐ 匹配模式

☒ 限速模式

请慎用限速模式，该模式访问控制策略只能添加一条

策略 每个源IP的访问速率 次/分钟

确定

取消

5. 单击 **URL 白名单**、**IP 白名单**或 **IP 黑名单**页签，进行黑白名单配置，支持添加、删除。

① 说明：

DDoS 高防包添加 URL 白名单时，可以带 HTTP 协议头信息，也可以不带 HTTP 协议头信息，但 DDoS 高防包仅支持 HTTP 协议。例如可以填写 `http://test.com/index.php` 或 `www.test.com/index.php`。

配置智能调度

最近更新时间：2024-11-08 09:20:52

应用场景

一般每个账号下可能拥有多个高防实例，且每个高防实例至少拥有一条高防线路，因此每个账号下可能会存在多条高防线路。当将业务添加至高防实例进行防护后，表示您已经为该业务配置一条高防线路作为防护线路。若您的业务配置存在多条高防线路作为防护线路，您需要考虑该业务流量的调度方式，即如何将业务流量调度到最优的高防线路进行防护，保证业务访问速度和高可用性。

目前 DDoS 防护服务提供优先级方式的 CNAME 智能调度功能，您可以根据实际需要，勾选高防实例并设置高防线路的优先级。

① 说明：

支持设置解析的高防实例有 DDoS 高防包、DDoS 高防 IP 和 DDoS 高防 IP 专业版，其中 DDoS 高防包包括独享包和共享包。

优先级调度方式

指针对所有的 DNS 请求均以优先级最高的高防线路进行响应，即所有访问流量被调度至当前优先级最高的高防线路。您可以编辑高防线路的优先级，默认优先级为100，优先级的值越小，则表示该高防线路优先级越高。具体调度规则如下：

- 如果业务配置的高防实例包含多条不同高防线路，且优先级相同时，则按照 DNS 请求的运营商来源进行响应。当其中某条高防线路遭遇封堵后，将按照 BGP > 电信 > 联通 > 移动 > 境外（包括中国香港、中国台湾）的线路顺序进行调度。
- 如果同一优先级的高防线路均遭遇封堵后，访问流量将自动调度到当前可用的优先级次高的高防线路。

① 注意：

若当前无次高优先级的高防线路可用，则无法进行自动调度，业务访问将会中断。

- 如果业务配置的高防实例，包含多条相同高防线路，且优先级相同时，则按负载均衡方式进行调度，将访问流量平均分发至这些相同运营商的高防线路上进行处理。

示例

假设您拥有高防实例：BGP 高防 IP 1.1.1.1和1.1.1.2、电信高防 IP 2.2.2.2、联通高防 IP 3.3.3.3，其中 1.1.1.1、2.2.2.2和3.3.3.3的优先级都为1，1.1.1.2的优先级为2。正常情况下，所有流量被调度至当前优先级为1的一组高防线路进行分发处理，因此来自联通的流量调度到3.3.3.3进行处理，来自电信的流量调度到 2.2.2.2进行处理，来自其他运营商的流量调度到1.1.1.1进行处理。当1.1.1.1进入封堵时，该 IP 下的访问流量将自动调度到 2.2.2.2进行处理，当1.1.1.1和3.3.3.3都被封堵时，则原本调度至1.1.1.1和3.3.3.3的访问流量，都将分发至 2.2.2.2进行处理，当该组高防线路全部进入封堵时，流量将被调度至1.1.1.2进行处理。

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。

① 说明：

- 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 高防包 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 高防 IP 接入非网站业务](#) 或 [接入网站业务](#)。

- 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 [云解析 DNS](#)。

设置线路优先级

请参考以下步骤，按照设想的调度方案为您的高防线路设置优先级：

- 登录 [DDoS 防护管理控制台](#)，在左侧导航栏选择智能调度 > 域名列表，进入域名列表页面，单击创建智能调度，系统自动生成一个 CNAME 记录。



- 找到该 CNAME 记录所在行，单击添加高防实例，进入智能调度编辑页面。



3. 在智能调度编辑页面中，TTL 值默认60秒，取值范围为1 – 3600（秒），调度方式为默认优先级。

智能调度编辑

CNAME

TTL值 60秒 [调整](#)

调度方式 优先级

IP资源和解析设置 [添加高防实例](#)

4. 进入添加高防实例页面，勾选需要设置高防线路优先级的实例，可选高防实例包括独享包、共享包、DDoS 高防 IP 和 DDoS 高防 IP 专业版，单击确定。

添加高防实例

选择IP

高防IP专业版

独享包

共享包

高防IP

高防IP专业版

输入ID/

资源类型

☐

net-00000025

高防IP专业版

☒

net-00000024

高防IP专业版

☐

net-00000024

高防IP专业版

☐

net-00000024

高防IP专业版

☐

net-00000024

高防IP专业版

☐

net-00000023

高防IP专业版

已选择(4)

资源ID/名称	IP地址	资源类型	
bgp-00000046		独享包	×
bgpip-00000101		高防IP	×
net-00000025		高防IP专业版	×
net-00000024		高防IP专业版	×

确定

取消

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。

智能调度编辑

CNAME4ion6w7a

TTL值60秒 [调整](#)

调度方式优先级

IP资源和解析设置 [添加高防实例](#)

资源ID	IP地址	线路	优先级	地区	运行状态	域名解析	操作
net-00000		BGP	100 ✎	华东地区(上海)	运行中	☒	解除绑定
net-00000		BGP	100 ✎	华东地区(上海)	运行中	☒	解除绑定
bgpip-00000		电信	100 ✎	华东地区(上海)	运行中	☒	解除绑定
bgp-00000		BGP	100 ✎	华东地区(上海)	运行中	☒	解除绑定

[确定](#) [取消](#)

示例

例如，您想要将业务流量先调度到 BGP 高防线路，当 BGP 高防线路被攻击遭到封堵后，将流量自动调度到电信高防线路。如果电信高防线路也被封堵，则将流量调度到联通高防线路。当 BGP 高防线路的封堵解除后，流量将自动恢复调度至 BGP 高防线路。

优先级设置方式：您可以将防护业务的高防实例中属于 BGP 高防线路的优先级设置成1、电信高防线路的优先级设置成2、联通高防 IP 线路的优先级不变，即可满足上述调度方案。

资源ID	IP地址	线路	优先级	地区	运行状态	域名解析	操作
net-00000		联通	100 ✎	华东地区(上海)	运行中	☒	解除绑定
bgpip-00000		电信	2 ✎	华东地区(上海)	运行中	☒	解除绑定
bgp-00000		BGP	1 ✎	华东地区(上海)	运行中	☒	解除绑定

如果您暂时不希望联通高防 IP 线路加入流量调度机制，单击  关闭域名解析即可，后面再根据需要重新开启域名解析并设置优先级。若想从当前调度机制中剔除该线路，可直接找到该线路对应实例所在行，单击[解除绑定](#)即可。

修改 DNS 解析

使用 CNAME 智能调度前，建议您将业务域名 DNS 的 CNAME 记录，修改为 DDoS 防护智能调度系统自动生成的 CNAME，使所有用户访问业务网站的流量都牵引至高防系统。

1. 登录腾讯云 [云解析 DNS 控制台](#)，在左侧导航栏中，单击**域名解析列表**，在域名解析列表页面，找到目标域名所在行，单击**解析**。

☐	域名	解析状态 ^①	解析套餐	最后操作时间	操作
☐		域名 DNS 未修改 ^①	个人专业版 2019-09-17 到期	2018-09-17 19:42:28	解析 升级套餐 更多 ▼
☐		域名 DNS 未修改 ^①	企业旗舰版 2020-01-22 到期	2018-01-22 11:13:50	解析 升级套餐 更多 ▼

2. 选择**记录管理 > 添加记录**，记录类型选择 CNAME，记录值内输入智能调度系统自动生成的 CNAME 地址，单击**保存**。

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

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 [↗](#)
请到域名注册商处将DNS修改为：ns3.dnsv5.com 或 ns4.dnsv5.com 后
修改DNS服务器需要最长72个小时的全球生效时间，请耐心等待。
遇到问题？查看FAQ文档 [↗](#)

添加记录

快速添加网站/邮箱解析 暂停 开启 删除 分配至项目

请输入您要搜索的记录

☐	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
☐	*	CNAME	默认	添加下提示类值	-	600	-	保存 取消

版权所有：腾讯云计算（北京）有限责任公司

第142 共285页

配置攻击告警阈值

最近更新时间：2023-07-21 09:44:37

应用场景

当您所使用的 DDoS 高防包遭受攻击、受攻击结束、被封堵以及解除封堵时，系统将以站内信、短信、邮件或微信的方式向您推送攻击告警信息。为更加合理、准确地推送攻击告警信息，减少困扰，新增攻击告警阈值配置功能。若检测的指标超过您设定的阈值，将触发告警，并向您推送攻击告警信息。若发生正常业务操作（如同步数据等）引起流量突增，但被判定为攻击的现象，该功能可以较好地过滤这类情况，帮助您更加准确、清晰地掌握当前业务遭受的攻击状况。如何接收告警信息，请参见 [设置安全事件通知](#)。

配置 DDoS 攻击告警阈值

本配置示例可实现如下功能：当高防系统检测到独享型高防包实例“bgp-000005w1”的入流量带宽超过 1000Mbps 时，将向指定用户群体发送 DDoS 攻击告警信息。

注意：
需要开启 DDoS 防护状态，才可设置攻击告警阈值。

1. 登录 [DDoS 防护控制台](#)，在左侧导航栏中，选择 **DDoS 高防包 > 资产列表**，进入 BGP 高防包页面，单击**独享包**，找到高防包实例“bgp-000005w1”，单击实例所在行的操作项**防护配置**。



2. 进入 DDoS 防护配置页面，在 DDoS 攻击告警阈值右侧的下拉框，选择告警指标**入流量带宽**，并设置阈值为 1000Mbps。

说明：
DDoS 攻击告警阈值默认未设置，支持可选的告警指标有入流量带宽和清洗流量。

DDoS防护配置

防护状态

☒

清洗阈值 ⓘ

默认

防护等级 ⓘ

宽松

正常

严格

业务场景

无

高级策略

无

DDoS攻击告警阈值

入流量带宽

1000

Mbps

配置 CC 攻击告警阈值

本配置示例可实现如下功能：独享型高防包实例“bgp-000006i9”触发 CC 防护后，当 CC 防护峰值超过 2000QPS 时，将向指定用户群体发送 CC 攻击告警信息。

① 注意：

需要开启 CC 防护状态，才可设置攻击告警阈值。

1. 登录 [DDoS 防护控制台](#)，在左侧导航栏中，选择 **DDoS 高防包** > **防护配置**，进入防护配置页面，选择**独享包** > **CC 防护**。
2. 开启 **CC 防护**，在 CC 攻击告警阈值处，设置阈值为2000QPS。

防护配置

独享包

DDoS防护

CC防护

DDoS高级防护策略

全部

bgp-000006i9/

CC防护

☒

对于敏感业务，可将业务URL添加到URL白名单，对该业务不做CC攻击检测和防护

http请求数阈值

3000 QPS

当http请求数超过设定值时，触发CC防护。

CC攻击告警阈值

2000

QPS

查看统计报表

最近更新时间：2025-08-07 17:59:42

将防护 IP 接入到 DDoS 高防包服务后，当用户收到 DDoS 攻击提醒信息或发现业务出现异常时，需要快速了解攻击情况，包括攻击流量大小、防护效果等，可在控制台进行查看。在掌握足够信息后，才可以采取更有效的处理方式，第一时间保障业务正常。

查看 DDoS 攻击防护情况

1. 登录 [DDoS 防护管理控制台](#)。
2. 定位到 **DDoS 高防包** > **统计报表**。选择**独享包**。

① 说明：

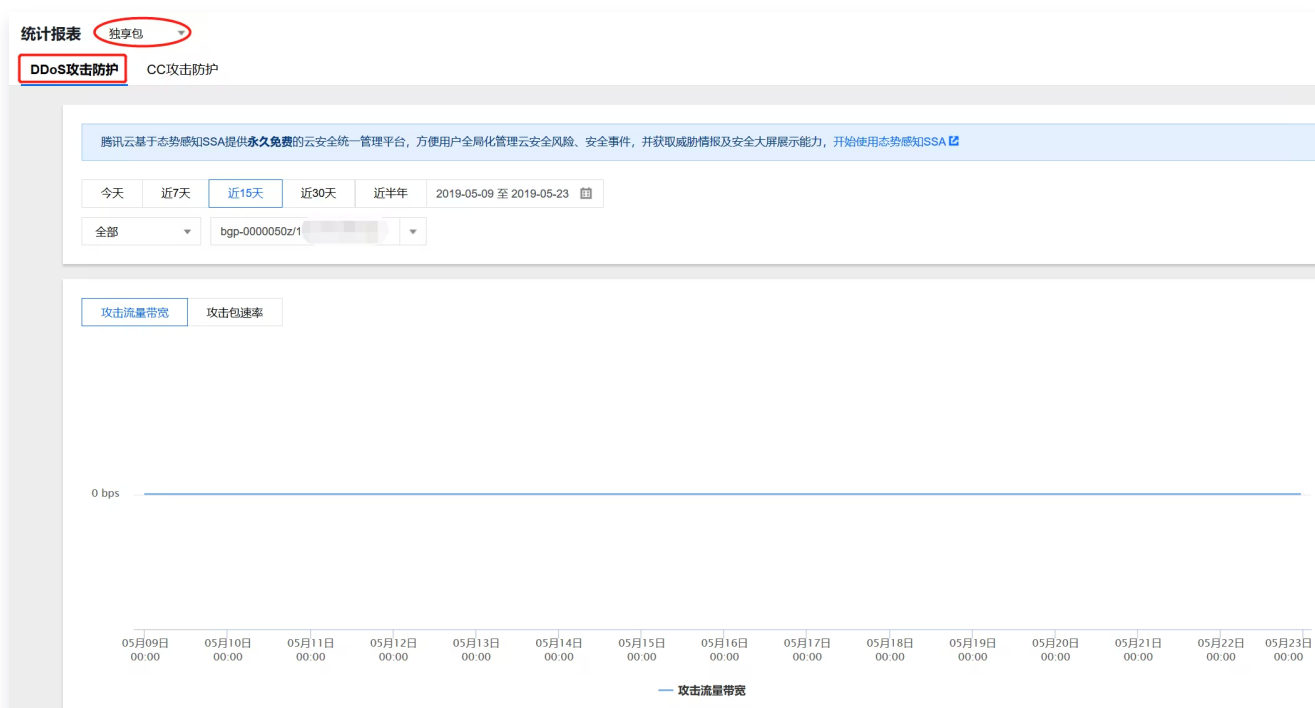
当选择**共享包**，可查看该类型高防包中每个防护 IP 的 DDoS 攻击防护情况。

3. 在**DDoS 攻击防护**页签，设置查询时间范围，选择目的地域和高防包实例，查看是否存在攻击。

① 说明：

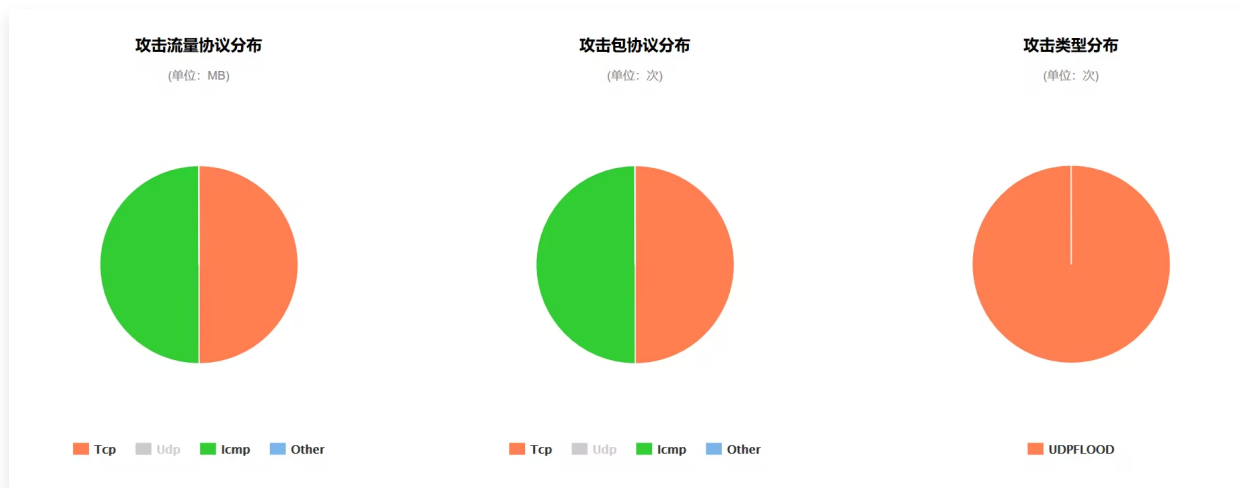
支持查询最多180天以内的攻击流量信息及 DDoS 攻击事件。

- 查看该时间范围内所选择的高防包防护遭受的攻击情况，包括网络**攻击流量带宽** / **攻击包速率**趋势。



- 通过攻击流量协议分布、攻击包协议分布和攻击类型分布，查看这三个数据维度下的攻击分布情况。
 - **攻击流量协议分布**：查看该时间范围内，所选择的高防包实例遭受攻击事件中各协议总攻击流量的占比情况。

- **攻击包协议分布**：查看该时间范围内，所选择的高防包实例遭受攻击事件中各协议攻击包总数的占比情况。
- **攻击类型分布**：查看该时间范围内，所选择的高防包实例遭受的各攻击类型总次数占比情况。



- 在“攻击来源分布”区域查看该时间范围内，所遭受 DDoS 攻击事件的攻击源在国内、全球的分布情况，便于用户清晰了解攻击来源情况，为进一步防护措施提供基础依据。



- 在“DDoS 攻击记录”区域查看该时间范围内，所遭受的 DDoS 攻击事件，了解每一次攻击事件的攻击（开始）时间、持续时间、攻击类型以及攻击状态。
- 支持攻击包下载，供用户进行 DDoS 攻击分析及溯源支撑。
- 单击攻击详情，了解 DDoS 攻击事件中的最大包速率、最大攻击流量带宽和总的清洗流量情况。
- 单击攻击源信息，查看该时间范围内，所遭受攻击的攻击源 IP 地址、来源地区、产生的攻击流量及攻击包量大小等信息。

① 注意：

攻击源信息为抽样数据，即随机抓包统计的数据，在攻击结束后大约2小时才会显示数据。

DDoS攻击记录

攻击时间	持续时间	攻击类型	攻击状态	操作
▶ 2019-08-03 12:08:00	2分钟	SYNFLOOD	攻击结束	攻击包下载 攻击详情 攻击源信息
▶ 2019-08-03 11:21:00	2分钟	SYNFLOOD	攻击结束	攻击包下载 攻击详情 攻击源信息

查看 CC 攻击防护情况

1. 登录 [DDoS 防护管理控制台](#)。
2. 定位到 **DDoS 高防包 > 统计报表**，选择独享包。

① 说明：

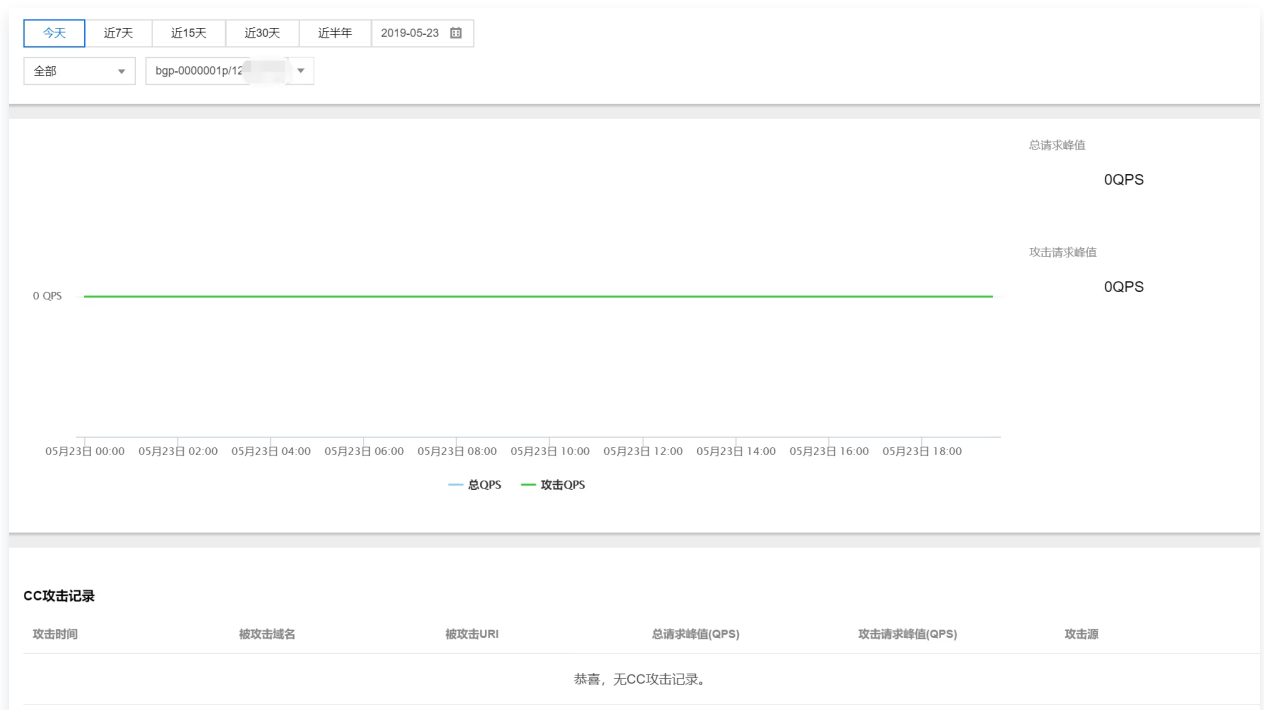
当选择**共享包**，可查看该类型高防包中每个防护 IP 的 CC 攻击防护情况。

3. 单击 **CC 攻击防护** 页签，设置查询时间范围，选择目的地域和高防包实例，查看是否存在 CC 攻击。

说明：

支持查询最多180天以内的攻击请求数信息及 CC 攻击事件。

- 用户可以选择**今天**查看所选高防包的攻击请求趋势。通过观察总请求量是否远高于正常业务访问量（QPS），以及攻击 QPS 是否存在且数值异常偏高。
- 如果存在 CC 攻击，系统会记录下攻击的开始时间、结束时间、被攻击域名、被攻击 URL、总请求峰值、攻击请求峰值和攻击源等信息。
 - **总请求峰值**：统计遭受攻击时，高防包接收到的总请求流量峰值。
 - **攻击请求峰值**：统计遭受攻击时，由高防系统阻断的请求次数峰值。



查看操作日志

最近更新时间：2023-07-21 09:44:37

操作场景

DDoS 高防包支持查看近90天内重要操作的日志，如有需要，您可以登录 [DDoS 防护管理控制台](#) 查看。可查看的日志包含以下类别：

- 防护对象 IP 更换日志
- DDoS 高级防护策略变更操作日志
- 清洗阈值调整日志
- 防护等级变更日志
- CC 防护策略变更操作日志
- 弹性防护峰值调整日志
- 资源名称的修改日志

操作步骤

1. 登录 [DDoS 防护管理控制台](#)。
2. 选择**操作日志**，进入操作日志查询页面。
3. 设置时间范围，通过**产品类型**筛选**独享包**或**共享包**，查看对应的操作记录。

说明：

- 独享包：指提供单个 IP 独享 DDoS 防护能力的 DDoS 高防包。
- 共享包：指提供多个 IP 共享 DDoS 防护能力的 DDoS 高防包。

操作日志

今天	昨天	近7天	近15天	近30天	2018-11-14 至 2018-12-13	请输入资源ID/账号
操作时间	对象ID	产品类型	操作内容	操作结果	操作账号	操作
2018-11-30 16:56:40		共享包	DDoS高级策略绑定资源	成功		展开
2018-11-30 16:56:24		共享包	DDoS高级策略绑定资源	成功		展开
2018-11-30 16:55:57		共享包	修改DDoS高级策略名称	成功		展开
2018-11-30 16:55:57		共享包	修改DDoS高级策略	成功		展开

设置安全事件通知

最近更新时间：2023-07-21 09:44:37

操作场景

当您使用的高防包防护 IP 受到攻击、受攻击结束、IP 被封堵以及解除封堵时，将以站内信、短信、邮件、微信或者电话的方式，向您推送告警信息：

- 攻击开始时，您将会收到攻击开始提示。
- 攻击结束后15分钟，您将收到攻击结束提示。
- IP 被封堵时，您将收到封堵提示。
- IP 解除封堵时，您将收到解除封堵提示。

您可以根据实际情况修改告警信息的接收人和接收方式。

操作步骤

1. 登录您的腾讯云账号，进入 [消息中心](#)。

① 说明：

您也可以登录 [控制台](#)，单击右上角的 ，在弹出页面单击[查看更多](#)，进入消息中心。

2. 在左侧目录中单击[消息订阅](#)，进入消息列表。
3. 在消息列表中，在安全事件通知所在列，选择接收方式，单击[修改消息接收人](#)，进入修改消息接收人页面。

添加接收人		移除接收人											
消息类型		☐ 站内信	☐ 邮件	☒ 短信	☐ 微信	☐ 企业微信	☐ 语音	接收人		操作			
▸ ☐ 财务消息													
▸ ☐ 产品消息													
▼ ☐ 安全消息													
☐ 安全事件通知		☒	☒	☒	☒	☐	☐	腾讯云安全技术支持		修改消息接收人			
☐ 产品遭受（如DDoS）攻击、服务器对外（如DDoS）攻击/扫描导致被隔离等安全事件的通知		☒	☒	☐	☐	☐	☐	腾讯云安全技术支持		修改消息接收人			

4. 在修改消息接收人页面，进行消息接收人的设置，设置完成后单击确定即可。

修改消息接收人

① 邮箱、手机、微信未验证的用户将无法接收邮件、短信、语音、微信消息，验证通过并开启对应接收方式后即可接收
非企业微信子用户无法接收企业微信消息，企业微信子用户且在腾讯云助手应用的成员可见范围内方可接收企业微信消息。

消息类型

安全事件通知

接收人

用户

用户组

新增消息接收人

修改接收人联系方式

搜索用户名称

Q

☒

用户名称

☐

用户类型

☐

手机号码

☐

邮箱

☐

微信

☒

1

已选择(1)

确定

取消

版权所有：腾讯云计算（北京）有限责任公司

第150 共285页

实践教程

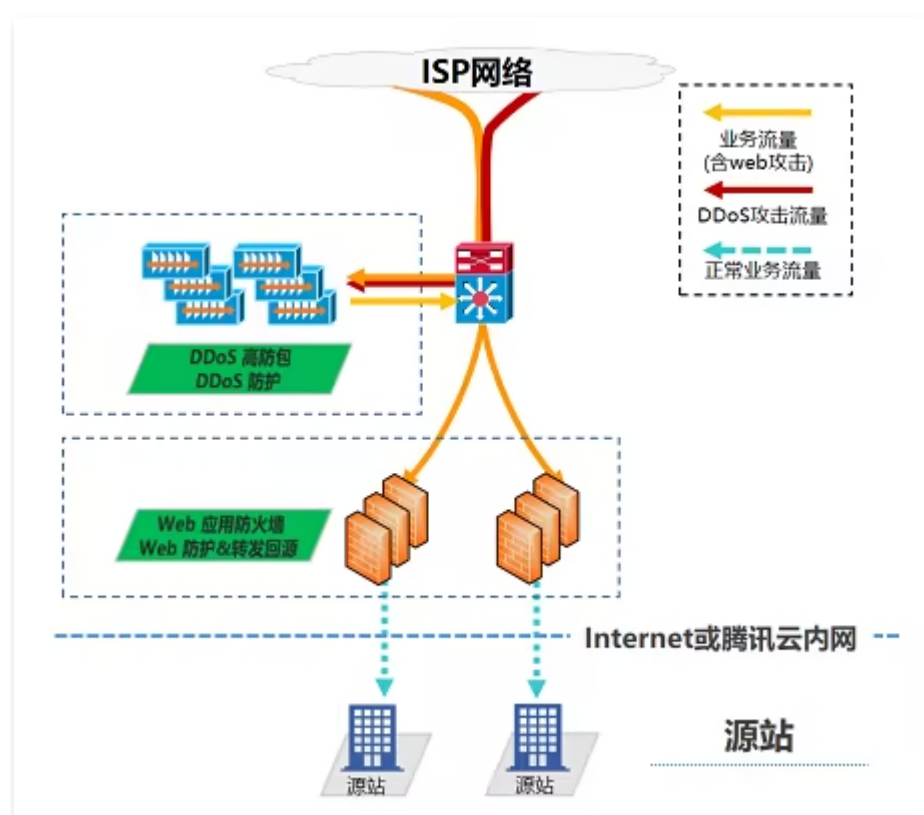
DDoS 高防包与 Web 应用防火墙结合使用

最近更新时间：2023-07-21 09:44:37

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

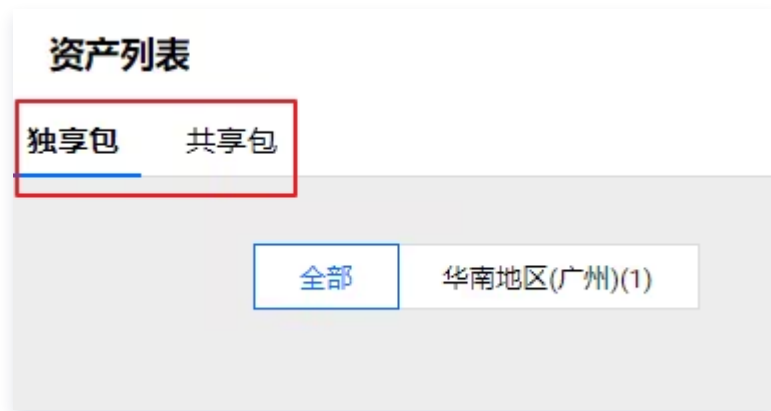
如需快速接入 Web 应用防火墙，详情请参见 [Web 应用防火墙快速入门](#)。

配置 DDoS 高防包

1. 登录 [DDoS 防护管理控制台](#)，在左侧导航中，选择 DDoS 高防包 > 资产列表。

- 若您的 DDoS 高防包实例是独享包，则选择独享包页签。

- 若您的 DDoS 高防包实例是共享包，则选择**共享包**页签。



2. 选择目的高防包实例所在地域，并在目的高防包实例所在行的右侧操作栏，单击**绑定设备**。



3. 在**绑定设备**页面，选择**关联设备类型**为**Web 应用防火墙**，设置**选择关联机器**为对应 Web 应用防火墙防护的 IP 地址。

① 说明：

共享包实例可绑定多个 Web 应用防火墙防护的 IP 地址。



4. 设置完成后，单击**确定**即可。

① 说明：

若是负载均衡型 Web 应用防火墙，在绑定界面选择**关联设备类型**为**负载均衡**，设置**选择关联机器**为对应负载均衡的公网 IP 地址。

DDoS 高防包异地防护方案

最近更新时间：2025-08-07 15:13:21

需求背景

受客观因素影响，DDoS 高防包在北京、上海和广州可售卖的最大防护能力有所差异，上海可售卖的最大防护能力为300Gbps，广州和北京两地可售卖防护能力均小于上海。除此之外，中国内地（大陆）成都、重庆等区域尚未上线高防包产品。

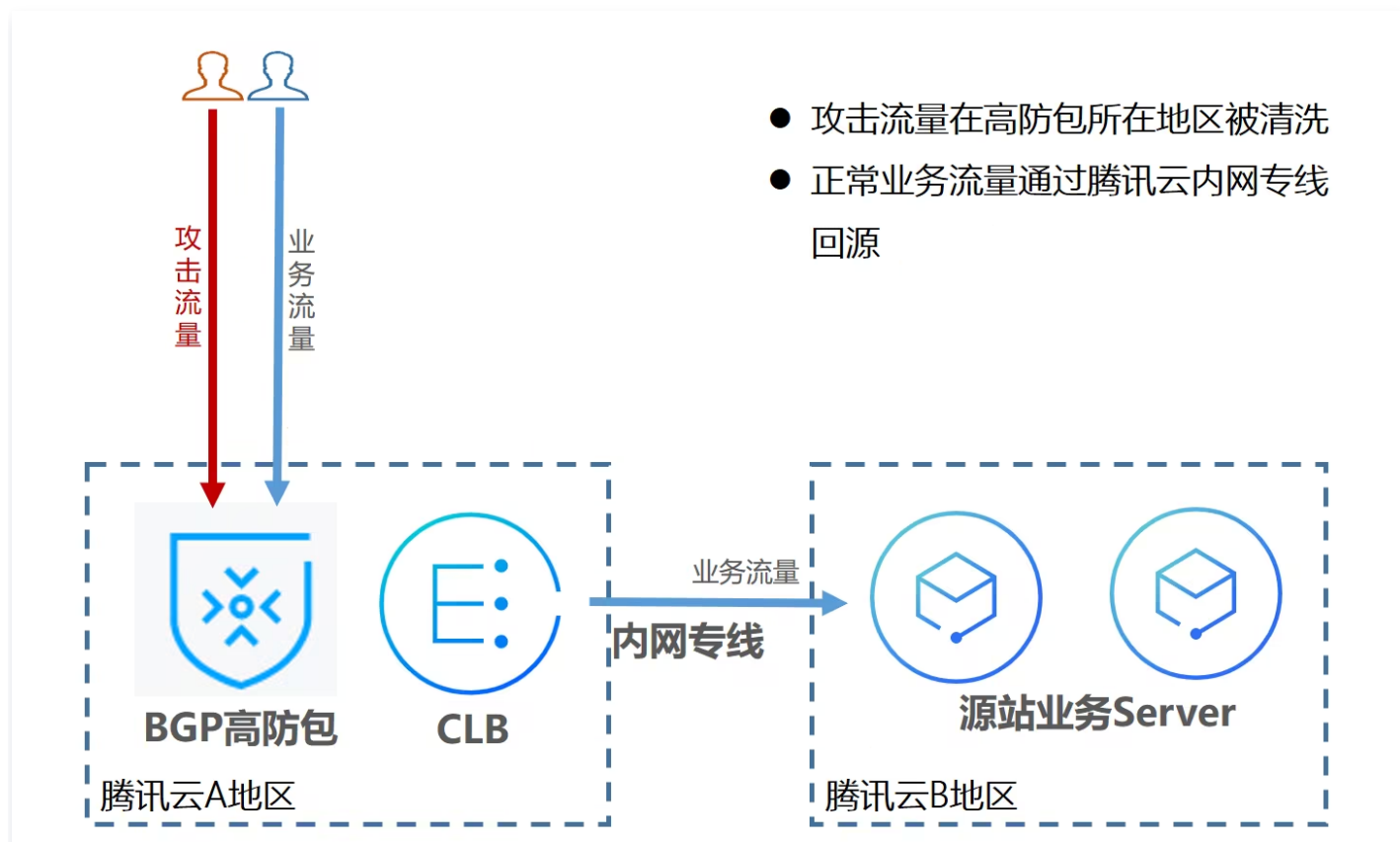
如果用户业务源站部署在腾讯云，并且需要使用腾讯云非源站所在地区的 DDoS 防护能力时，可参考本方案。

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300Gbps的 DDoS 高防包 DDoS 防护能力。
- 业务流量使用腾讯云的内地网专线进行转发，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。

业务系统压力测试建议

最近更新时间：2023-07-21 09:44:38

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。

① 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。

① 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。

SDK 文档

水印 SDK

最近更新时间：2025-08-08 14:31:52

本文将为您介绍如何接入水印 SDK，本文主要包括 Android、iOS 和 Windows 三个版本的接入指南。

SDK 准备

下载相关 [Demo](#) 及 [SDK](#)。

Android 接入

预备工作

- 接入 SDK 需要完成以下步骤：
 - 1.1 根据运行平台选择相应的 so 文件，将 so 文件和 jar 文件拷贝到工程目录下并添加依赖。
 - 1.2 调用 SDK 接口函数，生成水印信息。
 - 1.3 发送报文时，将20字节水印信息放在消息体前面。
- SDK 文件包含 so 文件和 jar 文件，目录结构如下：



- SDK API 说明：
 - 程序包：com.gamesec
 - 类：Mark
- 接口说明：

接口名称	说明
CreateSDKBuffFromStr	生成水印

接入步骤（Android Studio）

1. 将 sdk/android 文件夹下的内容拷贝到工程目录的 libs 文件夹下:



2. 修改项目的 build.gradle 文件, 设置 jni 文件目录, 添加 jar 依赖:

```
android {  
    sourceSets {  
        main {  
            jniLibs.srcDirs = ['libs/jni'] // 设置 jni 目录  
        }  
    }  
    dependencies {  
        implementation files('libs/gamesec.jar') // 添加依赖  
    }  
}
```

3. Eclipse 接入方法类似, 不需要配置 build.gradle 文件。

接口调用

1. 导入程序包。

```
import com.gamesec.*;
```

2. 实例化 Mark 对象。

```
Mark mark = new Mark();
```

3. 调用 CreateSDKBuffFromStr 生成水印。

```
byte [ ] CreateSDKBuffFromStr (String pSDKinfo, String buffer, String  
uDesIp, int uDesPort)
```

● 参数说明:

参数	类型	含义
----	----	----

pSDKInfo	String	水印防护密钥
buffer	String	占位参数，传入空字符串即可
uDesIp	String	服务器 IP，如 “1.2.3.4”
uDesPort	int	服务器端口

- 返回值：

类型	含义
byte[]	计算的水印信息，取20字节

- 调用示例：

```
String pSDKInfo = "566c2dea9420eb37-b6c8-566c2dea9420eb3710525135e8485e80806a2f9c";
String uDesIp = "115.159.147.198";
int uDesPort = 8899 ;
byte[] bytes = mark.CreateSDKBuffFromStr(pSDKInfo, "", uDesIp, uDesPort);
```

4. 添加水印信息到消息体。代码示例如下：

```
Socket s = new Socket(uDesIp, uDesPort);
OutputStream out = s.getOutputStream();
PrintWriter output = new PrintWriter(out, true);
// 先传入水印信息
output.print(bytes);
output.println("msg msg msg");
BufferedReader input = new BufferedReader(new InputStreamReader(s.getInputStream()));
String msg = input.readLine();
s.close();
```

iOS 接入

预备工作

- 接入 SDK 需要完成以下步骤：

1.1 将 SDK 文件拷贝到工程目录，Swift 工程需要添加桥文件。

1.2 调用 SDK 接口函数，生成水印信息。

1.3 发送报文时，将 20 字节水印信息放在消息体前面。

- SDK 文件包含 a 文件和 h 文件，目录结构如下：

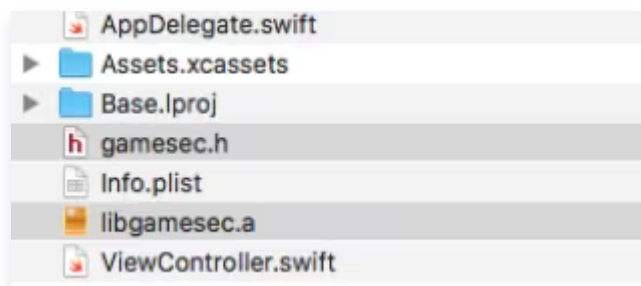


- 接口说明：

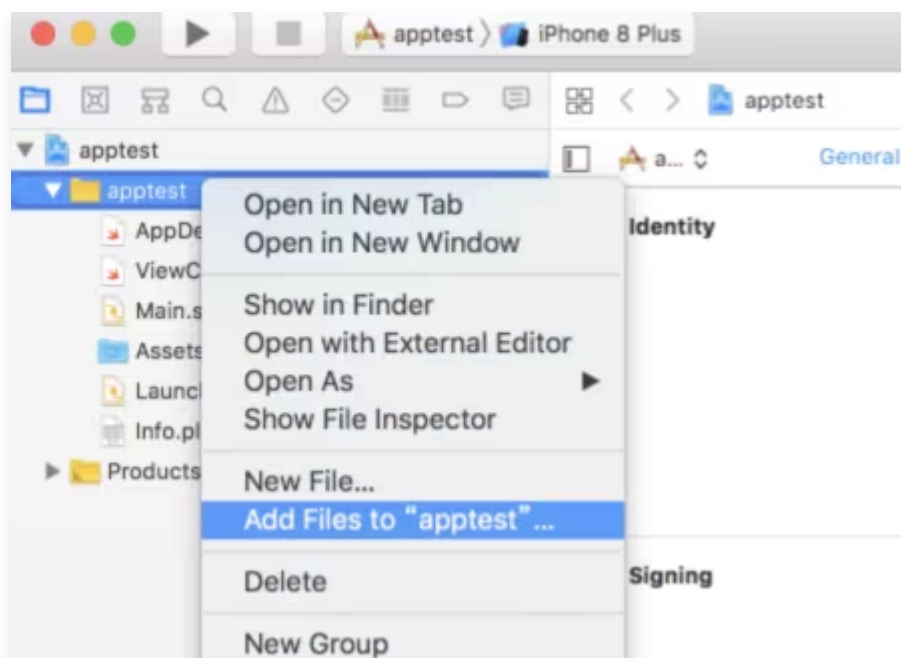
接口名称	说明
CreateSDKBuffFromStr	生成水印

接入步骤（Xcode）

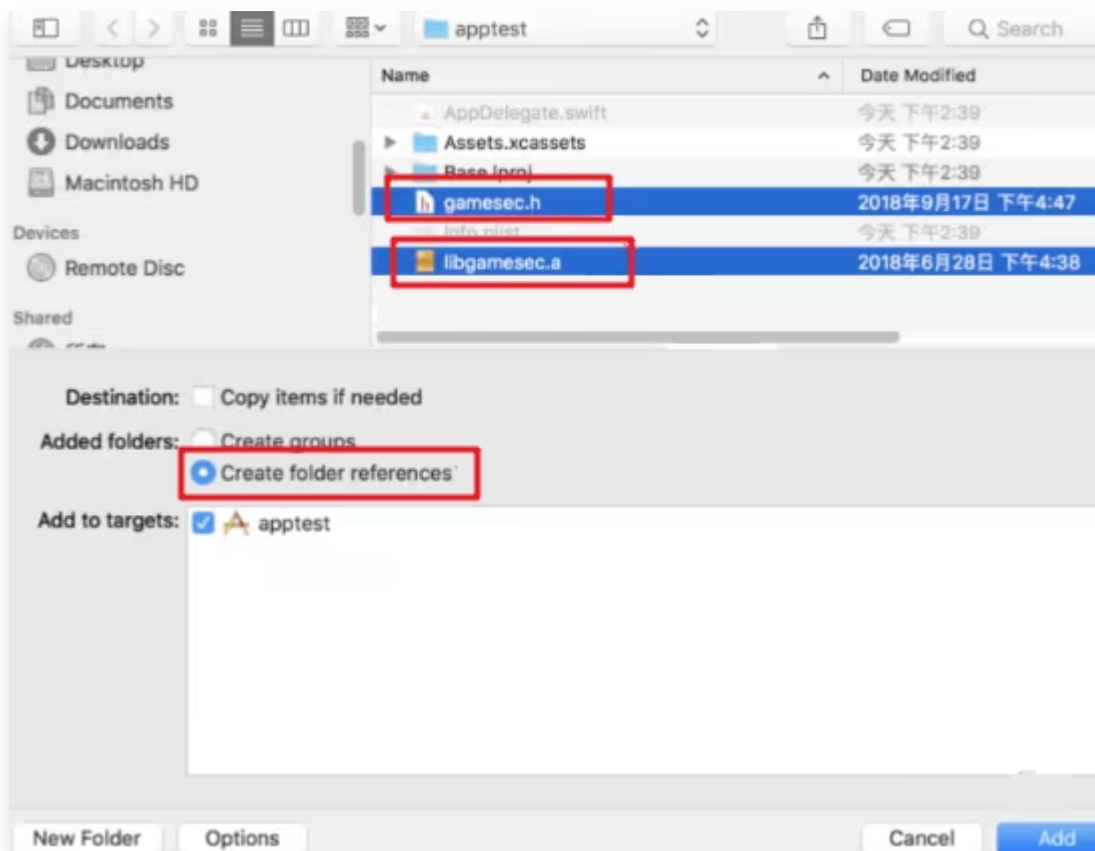
- 将 sdk/ios 文件夹下的内容拷贝到工程目录：



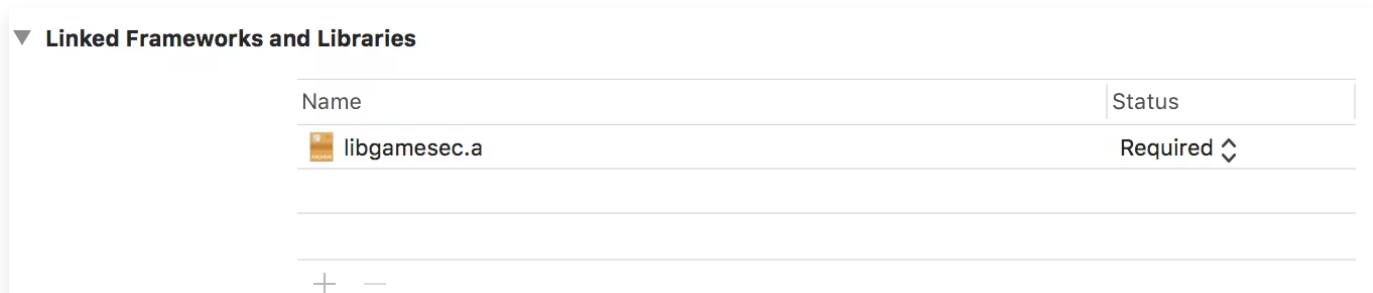
- 将 SDK 文件添加到 Xcode。右键工程名，单击“Add Files to”。



3. 在对话框中勾选 “Create folder references”，选中 SDK 的两个文件，单击 **Add**。



4. 左键工程名，选择 General，将 a 文件添加到 “Linked Frameworks and Libraries”：

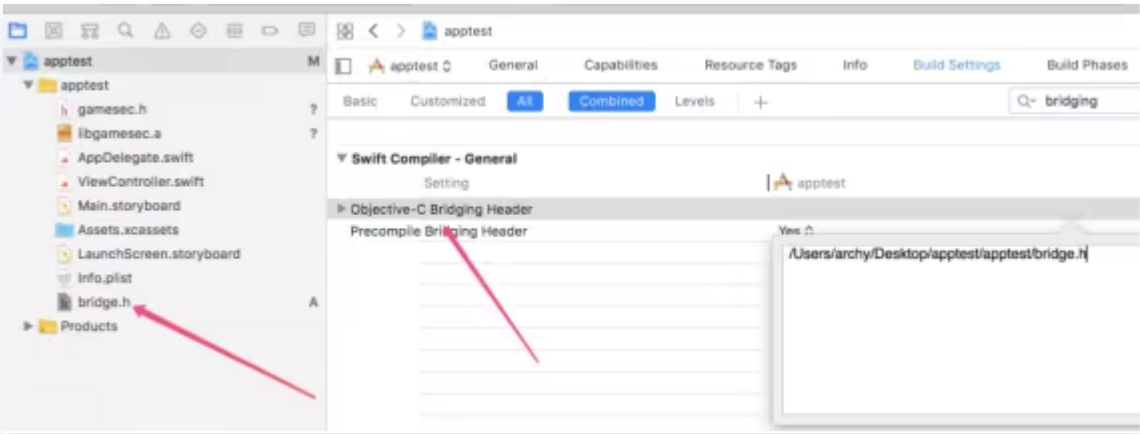


5. 如果是 Swift 项目，需要创建桥文件，Objective-C 项目可以跳过此步骤。创建一个 Header File，命名为 bridge.h。并在文件中添加以下代码：

```
# import "gamesec.h";
```

6. 左键工程名，选择 Build Settings，将 bridge.h 添加到 Objective-C Bridging Header 中：

7.



接口调用

1. Swift 项目可以直接调用生成水印函数，Objective-C 项目需要在使用的文件里面添加头文件：

```
# import "gamesec.h";
```

2. 调用 CreateSDKBuffFromStr 生成水印。

```
uint32_t CreateSDKBuffFromStr(char *pSDKInfo, uint8_t *buffer, char*
uDstIp, uint16_tuDstPort);
```

参数说明：

参数	类型	含义
pSDKInfo	char *	水印防护密钥
buffer	uint8_t *	水印指针，输出水印结果
uDesIp	char *	服务器 IP，如 “1.2.3.4”
uDesPort	uint16_t	服务器端口

① 注意：

水印结果保存在参数 buffer 中，取20字节。

3. 调用示例。

```
Swift 调用：
let pSDKInfo = UnsafeMutablePointer<Int8>(mutating: (
```

```
        "566c2dea9420eb37-b6c8-  
566c2dea9420eb3710525135e8485e80806a2f9c"  
        as NSString).utf8String);  
        var buffer =  
UnsafeMutablePointer<UInt8>.allocate(capacity: 20);  
        let uDstIp = UnsafeMutablePointer<Int8>(mutating: (  
        "115.159.147.198" as NSString).utf8String);  
        let uDstport = UInt16.init("8899")!;  
  
        CreateSDKBuffFromStr(pSDKInfo, buffer, uDstIp, uDstport);  
  
        for i in 0 ..< 20 {  
            let b = (buffer+i).pointee;  
            // 水印信息在前20字节，注意这里输出的是 uint8  
            print(" \ (b) ");  
        }
```

Object-C 调用:

```
char *pSDKInfo = "566c2dea9420eb37-b6c8-  
566c2dea9420eb3710525135e8485e80806a2f9c";  
uint8_t buffer[20];  
char *uDstIp = "115.159.147.198";  
uint16_t uDstPort = 8899;  
  
CreateSDKBuffFromStr(pSDKInfo, buffer, uDstIp,  
uDstPort);  
  
for(int i=0;i<20;i++)  
{  
    // 水印信息在前20字节  
    NSLog(@"%d", (int8_t)buffer[i]);  
}
```

3. 发送报文前，添加 20 字节水印信息到消息体前面。

Windows 接入

预备工作

SDK 为 gamesec.dll 文件，有一个生成水印的函数：

```
uint32_t CreateSDKBuffFromStr(char *pSDKInfo, uint8_t *buffer, char*
uDstIp, uint16_t uDstPort);
```

参数说明:

参数	类型	含义
pSDKInfo	char *	水印防护密钥
buffer	uint8_t *	水印指针，输出水印结果
uDesIp	char *	服务器 IP，如 “1.2.3.4”
uDesPort	uint16_t	服务器端口

① 说明:

水印结果保存在参数 buffer 中，取20字节。

接口调用

在使用水印函数时，需先导入 dll 文件，可以使用 LoadLibrary 函数（需要添加 Windows.h）：

```
// 定义函数指针
typedef int(*FUNC)(char *, uint8_t *, char* , uint16_t );
// 设置 dll 路径
HINSTANCE Hint = ::LoadLibrary(L"E:\\sdk\\gamesec.dll");
FUNC CreateSDKBuffFromStr = (FUNC)GetProcAddress(Hint,
"CreateSDKBuffFromStr");
```

完整调用示例:

```
// 保存水印
uint8_t buffer[BUFFER_SIZE];
memset(buffer, 0, BUFFER_SIZE);

int UDP_TEST_PORT = 8899;

const char * CONST_UDP_SERVER_IP = "115.159.147.198";
char * UDP_SERVER_IP = new char[strlen(CONST_UDP_SERVER_IP)];
strcpy(UDP_SERVER_IP, CONST_UDP_SERVER_IP);
```



```
const char * CONST_pSDKInfo =
"566c2dea9420eb37-b6c8-566c2dea9420eb3710525135e8485e80806a2f9c";
char * pSDKInfo = new char[strlen(CONST_pSDKInfo)];
strcpy(pSDKInfo, CONST_pSDKInfo);

// 调用10次
for (int i = 0; i < 5; i++) {
    CreateSDKBuffFromStr(pSDKInfo, buffer, (char *)UDP_SERVER_IP,
UDP_TEST_PORT);

    for (int i = 0; i <= 20; i++)
    {
        // 水印在前20字节
        printf("%d ", (int8_t)buffer[i]);
    }
    printf("\n\n");
}
```

常见问题

封堵相关问题

最近更新时间：2023-07-21 09:44:38

DDoS 高防包所防护的 IP 被封堵了该怎么办？

如果正使用的 DDoS 高防包实例未调整到最高弹性防护峰值，可以在 DDoS 高防包管理控制台中更改 DDoS 高防包实例的弹性防护峰值，提升弹性防护能力，抵御更大的攻击流量。

另外，使用 DDoS 高防包的用户每天将拥有三次自助解封机会，可在紧急情况下，进行 [自助解封](#)。

为什么进行封堵？

腾讯云通过共享基础设施的方式降低用云成本，所有用户共享腾讯云的外网出口。当发生大流量攻击时，除了会影响被攻击对象，整个腾讯云的网路都可能受到影响。为了避免攻击影响到其他未被攻击的用户，保障整个云平台网络的稳定，需要进行封堵。

为什么不提供免费无限抗攻击？

DDoS 攻击不仅影响受害者，也会对整个云网络造成严重影响，影响云内其它未被攻击的用户。DDoS 防御的成本非常高，一是带宽成本，二是清洗成本。其中最大的成本就是带宽费用，带宽费用以总流量计算，不会考虑是正常流量或是攻击流量而区别收费。

因此，腾讯云在成本可承受的范围内为云服务用户提供免费的 DDoS 基础防护服务，当攻击流量超出免费防护阈值时，腾讯云会屏蔽被攻击 IP 的外网流量。

为什么不能立即解除封堵？

通常 DDoS 攻击会持续一段时间，不会在封堵后立即停止，具体持续时间不定，腾讯云安全团队会根据大数据分析的结果，设定默认封堵时长。

由于封堵是在运营商网络部分生效，被攻击外网 IP 进入封堵后，腾讯云无法监控到攻击流量是否停止。如果在攻击未停止的情况下解除封堵，被攻击外网 IP 将再次进入封堵，同时在解除封堵至再次封堵生效的这段时间内，攻击流量将直接进入腾讯云的基础网络，可能会影响到云内其它客户。另外，封堵是腾讯云向运营商购买的服务，解封次数、频率都有限制。

紧急情况下，通过哪些途径可以提前解封？

1. 升级保底容量后，可自动提前解封。
2. 使用 DDoS 高防包的用户每天将拥有三次自助解封机会，可在紧急情况下，进行 [自助解封](#)。

为什么自助解封会有次数限制？有哪些限制？

封堵是腾讯云向运营商购买的服务，而运营商有明确的封堵解除时间和频率限制，所以封堵状态无法频繁手动解除。使用 DDoS 高防包的用户每天将拥有三次自助解封机会，当天超过三次后将无法进行解封操作。系统将在每天零点

时重置自助解封次数，当天未使用的解封次数不会累计到次日。

如何连接已被封堵的服务器？

如需进行数据迁移等操作，可参考以下两种方式连接已被封堵的服务器：

- 通过同地域的其它云服务器通过内网 IP 连接被封堵服务器。
- 通过 [云服务器控制台](#)，在被封堵服务器所在行，单击登录即可通过浏览器 VNC 方式连接。

怎样预防被封堵？

购买 [DDoS 高防包](#) 时，可根据历史攻击流量数据，选择适当的防护峰值，尽可能地确保最大防护峰值大于攻击峰值。

怎样避免解封后再次被封堵？

建议您升级保底防护峰值或弹性防护峰值，提高防御能力。开启弹性防护可帮您抵御大规模流量攻击，且弹性防护按天按量灵活付费，有效节约您的安全成本。

功能相关问题

最近更新时间：2023-07-21 09:44:38

DDoS 高防包支持腾讯云外的 IP 接入防护吗？

不支持。DDoS 高防包仅对腾讯云内的公网 IP 提供 DDoS 防护支持。如需腾讯云外的防护，请 [购买 DDoS 高防 IP](#)。

腾讯云内服务器有 DDoS 防御吗？

目前用户只要购买了腾讯云内服务器，默认对其设备绑定的公网 IP 开启 DDoS 基础防护：普通用户默认可享受 2Gbps 防护，VIP 用户可享受 10Gbps 防护。若需获得更大的 DDoS 防御能力，建议购买腾讯云的 [DDoS 高防包](#) 产品或 [DDoS 高防 IP](#) 产品。

如果绑定的资源已过期，DDoS 高防包实例还未过期，会怎么样？

DDoS 高防包实例是按月购买的，且以 IP 为媒介提供防护能力。如果绑定的防护对象资源过期，不及时更换 DDoS 高防包实例所绑定的 IP，那么该 DDoS 高防包实例在有效期内会持续为已绑定的 IP 提供防护，但该 IP 对应的资源不一定是您的。建议您及时为腾讯云服务续费，或更换新的防护对象 IP。

DDoS 高防包支持域名的防护吗？

不支持。若有域名防护以及应用层的防护需求，请 [购买 DDoS 高防 IP](#)。

DDoS 基础防护的防护带宽是 2Gbps，又购买了 DDoS 高防包的套餐，最终的防护峰值是否会叠加？

用户享有的最终防护峰值，以 DDoS 高防包购买套餐里的防护峰值为准，不会叠加 DDoS 基础防护的默认防护带宽。

假设某腾讯云服务器的 IP 原本享有 2Gbps 的免费防护带宽。因经常遭受攻击，用户又为该 IP 购买了 20Gbps 的 DDoS 高防包套餐，则最大防护能力为 20Gbps。

DDoS 高防包和 DDoS 高防 IP 的区别是什么？

- 防护对象：
 - DDoS 高防包只针对腾讯云内的服务提升 DDoS 防护能力。
 - DDoS 高防 IP 面向腾讯云外用户，为非腾讯云的业务 IP/域名提供防护。
- 接入：
 - DDoS 高防包的接入配置更加便捷，无需变更公网 IP 地址。
 - DDoS 高防 IP 需修改 DNS 解析或修改业务 IP 后才能接入防护。

DDoS 高防包与三网高防的区别是什么？

差异点	DDoS 高防包	三网高防
接入成本	无需更换服务器 IP，直接为腾讯云产品提升防御能力，即时生效，接入成本低	需要将服务器 IP 更换为三网 IP，填写域名与端口信息，配置相当复杂
访问质量	采用 BGP 带宽，减少跨网访问延迟，访问速度提升30%以上	无 BGP 带宽，网络延迟大，质量不佳
定价策略	计费灵活，支持保底+弹性，可共享	计费复杂，需要付流量费

计费相关问题

最近更新时间：2023-07-21 09:44:38

高防服务的弹性防护计费模式是否一样？如何计算的？

一样，都是按照当日可防护的攻击流量峰值对应弹性防护峰值区间进行计费，计费详情请参考 [计费概述](#)。

例如，您购买的 DDoS 高防包实例规格是20Gbps保底防护峰值 + 50Gbps弹性防护峰值。如果当天发生 DDoS 攻击事件且最高攻击流量峰值为45Gbps。45Gbps已超过保底防护峰值范围触发弹性防护，且属于40Gbps < 弹性峰值 ≤ 50Gbps计费区间，当天产生弹性费用按照40Gbps < 弹性峰值 ≤ 50Gbps计费区间收取。

如果 DDoS 高防包所防护的 IP 因遭受大流量攻击被封堵，该部分攻击流量是否会列入计费？

DDoS 高防包服务的弹性防护计费规则是针对超出保底防护峰值且小于等于弹性防护峰值的攻击流量进行计费。被封堵即意味着攻击流量已超过所设置的弹性防护峰值，因此超出弹性防护峰值的部分攻击流量不在计费范围内。

购买弹性防护后，如果一个月都没有遭受攻击，是否需要费用？

这种情况下，您只需要支付保底防护的包月费用即可，不产生其它额外的费用。

若购买了100Gbps的保底防护，是否可以降到50Gbps？

不可以。保底防护级别仅支持升级，不支持降级。

业务遭受攻击过程中，是否支持升级弹性防护峰值？

支持。DDoS 高防包服务基础信息界面支持调整弹性防护峰值，支持调升也支持调降。不同地域支持的防护能力不同，弹性防护峰值的具体取值范围请参考 [使用限制](#)。

① 注意：

若当日发生的攻击已经产生计费，修改后次日将以最新的弹性防护峰值进行计费。

受防护的 IP 一天之内遭受多次攻击，是否需要收取多次费用呢？

DDoS 高防包服务是以当日防护的最高攻击流量峰值来计算，只收取一次费用。

如果购买了两个高防服务套餐，且两个高防服务实例遭受的攻击流量都超过保底防护，如何收取弹性防护费用？

弹性防护费用以产品实例为计算单位，如果两个高防服务实例都超过保底防护，则需要分别收取两个高防实例的弹性防护费用。

DDoS 高防 IP（旧版）

产品简介

产品概述

最近更新时间：2025-08-07 17:59:42

简介

DDoS 高防 IP 是针对游戏、互联网及金融等业务遭受大流量 DDoS 攻击导致用户服务不可用的情况而推出的付费防护服务。用户通过配置高防 IP，将攻击流量引流到高防 IP 进行清洗，确保源站业务的稳定可用。

DDoS 高防 IP 使用公网代理的接入方式，支持 TCP，UDP，HTTP，HTTPS 和 HTTP2 等协议，覆盖金融、电商、游戏等各类业务。

主要功能

多类型防护

防护分类	描述
畸形报文过滤	过滤 frag flood，smurf，stream flood，land flood 攻击，过滤 IP 畸形包、TCP 畸形包、UDP 畸形包
网络层 DDoS 攻击防护	过滤 UDP Flood、SYN Flood、TCP Flood、ICMP Flood、ACK Flood、FIN Flood、RST Flood、DNS/NTP/SSDP 等反射攻击、空连接
应用层 DDoS 攻击防护	过滤 CC 攻击和 HTTP 慢速攻击，支持 HTTP 自定义特征过滤如 host 过滤、user-agent 过滤、Referer 过滤

高级防护策略灵活

DDoS 高防 IP 默认提供基础安全策略，策略基于 IP 画像、行为模式分析、AI 智能识别等防护算法，有效应对常见 DDoS 攻击行为。同时提供 DDoS 高级防护策略，用户可针对自身业务需求配置，通过 IP 黑白名单、禁用协议/端口、报文特征过滤策略、空连接防护等操作，提供针对性防护。

清洗模式自定义

开放多套防护等级，提供自定义清洗阈值，用户可根据攻击情况灵活调整，对不同类型的 DDoS 攻击快速响应，充分匹配不同用户不同业务类型。

防护统计及分析

提供 DDoS 攻击、CC 攻击、转发流量等多维度数据的统计与展示，帮助用户实时掌握业务和攻击情况。同时支持对攻击自动抓包，方便用户快速定位异常问题。

支持的地域

DDoS 高防 IP 可防护任何公网服务器，包括但不限于 IDC 机房、腾讯云、其他的云。目前已开放 DDoS 高防 IP 的地域包括：

- 中国内地（大陆）区域：华南地区（广州）、华东地区（上海）和华北地区（北京）。
- 境外区域：中国港澳台地区（香港、台湾）、亚太地区（新加坡、首尔、曼谷、日本）、美国东部（弗吉尼亚）、欧洲地区（法兰克福）。

DDoS 高防 IP 在不同地域提供的高防能力请参考如下表格：

地区	保底防护	弹性防护	最大防护能力
广州	20Gbps – 50Gbps	30Gbps – 100Gbps	100Gbps
北京	20Gbps – 50Gbps	30Gbps – 100Gbps	100Gbps
上海	20Gbps – 100Gbps	30Gbps – 300Gbps	300Gbps
境外区域	10Gbps – 100Gbps	30Gbps – 400Gbps	400Gbps

① 说明：

建议选择最靠近业务源站的地域，可降低访问时延、提高访问速度。

产品优势

最近更新时间：2023-07-21 09:44:39

DDoS 高防 IP 是腾讯云针对云外用户业务在遭受大流量 DDoS 攻击后导致服务不可用时推出的付费产品，其产品优势如下：

超大防护资源

- 腾讯云 BGP 链路对接全国各地30家运营商，单客户单点可提供高达900Gbps的防护能力。
- 境外数十个防护节点，高达400Gbps防护能力，轻松应对各类 DDoS 攻击。

领先的清洗能力

依托腾讯自研防护集群，采用 IP 画像、行为分析、Cookie 挑战等多维算法，并通过 AI 智能引擎持续更新防护算法，精准快速检测业务流量，灵活应对各类攻击行为。

极速访问体验

腾讯云 BGP 链路对接全国各地30家运营商，覆盖面广，能有效解决访问时延问题，保障各类用户群的访问速度，带来极速访问体验。

隐藏用户源站

DDoS 高防 IP 服务可对用户源站进行替换并隐藏。使用高防 IP 作为源站的对外服务地址，所有业务访问流量都经过高防 IP，将正常访问流量转发到源站，攻击流量在高防 IP 上被清洗后将干净流量返回给源站，增加源站安全性。

全业务支持

DDoS 高防 IP 服务支持网站和非网站业务，覆盖金融、电商、游戏、政府等各类业务，充分满足用户不同业务的安全防护需求。

定价灵活，优化成本

提供“保底防护+弹性防护”相结合计费方式，为用户降低日常安全费用，在需要时按需调整弹性防护，无需新增任何设备，无需调整配置。当攻击流量超过保底防护峰值时，腾讯云仍为用户继续防护，保障业务不中断，按当天实际攻击量付费。

丰富的攻击防护报表

提供精准的防护流量报表及攻击详情信息，使用户及时了解攻击实况。支持对攻击自动抓包，方便事后进行分析以及溯源。

应用场景

最近更新时间：2023-07-21 09:44:39

游戏

游戏行业是 DDoS 攻击的重灾区，DDoS 高防 IP 能有效保证游戏的可用性和持续性，保障游戏玩家流畅体验。同时为活动、新游戏发布或节假日游戏收入旺季时段保驾护航，确保游戏业务正常。

互联网

保证互联网网页的流畅访问，业务正常不中断。对电商大促等重大活动时段，提供安全护航。

金融

满足金融行业的合规性要求，保证线上交易的实时性、安全稳定性。

政府

满足国家政务云建设标准的安全需求，为重大会议、活动，敏感时期提供安全保障。保障民生服务正常可用，维护政府公信力。

企业

保证企业站点服务持续可用，避免 DDoS 攻击带来的经济及企业品牌形象损失问题。零硬件零维护，节省安全成本。

相关概念

最近更新时间：2023-07-27 11:17:12

DDoS 攻击

Distributed Denial of Service (DDoS)，即分布式拒绝服务攻击，指攻击者通过网络远程控制大量僵尸主机向一个或多个目标发送大量攻击请求，堵塞目标服务器的网络带宽或耗尽目标服务器的系统资源，导致其无法响应正常的服务请求。

网络层 DDoS 攻击

网络层 DDoS 攻击主要是指攻击者利用大流量攻击拥塞目标服务器的网络带宽，消耗服务器系统层资源，导致目标服务器无法正常响应客户访问的攻击方式。

常见攻击类型包括 SYN Flood、ACK Flood、UDP Flood、ICMP Flood 以及 DNS/NTP/SSDP/memcached 反射型攻击。

CC 攻击

CC 攻击主要是指通过恶意占用目标服务器应用层资源，消耗处理性能，导致其无法正常提供服务的攻击方式。

常见的攻击类型包括基于 HTTP/HTTPS 的 GET/POST Flood、四层 CC 以及 Connection Flood 等攻击方式。

防护峰值

防护峰值分为保底防护峰值和弹性防护峰值。

- 保底防护峰值：指高防服务实例的保底防护带宽能力，保底部分为按月预付费。
- 弹性防护峰值：指高防服务实例的最大弹性防护带宽能力，弹性部分为按天后付费。

若未开启弹性防护，则保底防护峰值为高防服务实例的最高防护峰值。若已开启弹性防护，则弹性防护峰值作为高防服务实例的最高防护峰值。当攻击流量超过高防服务实例的最高防护峰值后触发封堵。

① 说明：

弹性防护默认关闭。如需开启弹性防护，请在知悉弹性相关收费后自助开启。用户可以根据自身业务需求，随时调整弹性防护峰值。

弹性防护峰值的作用

开启弹性防护后，当攻击流量峰值超过购买的保底防护峰值且在弹性防护峰值范围内时，腾讯云 DDoS 高防 IP 可继续为用户提供防护，保障业务访问持续性。

弹性防护如何收费

开启弹性防护后，当攻击流量超过保底防护峰值时，会触发弹性防护并收取费用，取当天实际产生的最高攻击峰值所对应区间进行计费，账单次日生成。

例如，您购买的保底防护为20Gbps，且设置的弹性防护为50Gbps。若当天的实际攻击峰值为35Gbps，则需要支付30Gbps – 40Gbps区间的弹性防护费用。

详细费用请参见 [计费概述](#)。

清洗

当目标 IP 的公网网络流量超过设定的防护阈值时，腾讯云 DDoS 防护系统将自动对该 IP 的公网入向流量进行清洗。通过 BGP 路由协议将流量从原始网络路径中重定向到DDoS 防护系统的 DDoS 清洗设备上，通过清洗设备对该 IP 的流量进行识别，丢弃攻击流量，将正常流量转发至目标 IP。

通常情况下，清洗不会影响正常访问，仅在特殊场景或清洗策略配置有误时，可能会对正常访问造成影响。

封堵

当目标 IP 受到的攻击流量超过其封堵阈值时，腾讯云将通过运营商的服务屏蔽该 IP 的所有外网访问，保护云平台其他用户免受影响。简而言之，当您的某个 IP 受到的攻击流量超过您所购买的高防套餐最大 [防护峰值](#) 时，腾讯云将屏蔽该 IP 的所有外网访问。当您的防护 IP 被封堵时，您可以登录管理控制台 [自助解封](#)。

封堵阈值

DDoS 高防 IP 实例的防护 IP 的封堵阈值等于实际购买的最大 [防护峰值](#)。DDoS 高防 IP 有多种不同规格，详情请参考 [计费概述](#)。

封堵时长

封堵时长默认为2小时，实际封堵时长与封堵触发次数和攻击峰值相关，最长可达24小时。

封堵时长主要受以下因素影响：

- 攻击是否持续。若攻击一直持续，封堵时间会延长，封堵时间从延长时刻开始重新计算。
- 攻击是否频繁。被频繁攻击的用户被持续攻击的概率较大，封堵时间会自动延长。
- 攻击流量大小。被超大型流量攻击的用户，封堵时间会自动延长。

① 注意：

针对个别封堵过于频繁的用户，腾讯云保留延长封堵时长和降低封堵阈值的权利。

为什么进行封堵

腾讯云通过共享基础设施的方式降低用云成本，所有用户共享腾讯云的外网出口。当发生大流量攻击时，除了会影响被攻击对象，整个腾讯云的网路都可能会受到影响。为了避免攻击影响到其他未被攻击的用户，保障整个云平台网络的稳定，需要进行封堵。

为什么不提供免费无限抗攻击

DDoS 攻击不仅影响受害者，也会对整个云网络造成严重影响，影响云内其它未被攻击的用户。DDoS 防御的成本非常高，一是带宽成本，二是清洗成本。其中最大的成本就是带宽费用，带宽费用以总流量计算，不会考虑是正常流量或是攻击流量而区别收费。

因此，腾讯云在成本可承受的范围内为云服务用户提供免费的 DDoS 基础防护服务，当攻击流量超出免费防护阈值时，腾讯云会屏蔽被攻击 IP 的外网流量。

有关封堵的更多信息，请参见 [封堵相关问题](#)。

购买指南

计费概述

最近更新时间：2023-07-21 09:44:39

计费方式

DDoS 高防 IP 的计费方式为“保底防护峰值（预付费）+ 弹性防护峰值（后付费）+ 业务带宽（预付费）”。

计费项	计费模式	付费方式	付费说明
保底防护峰值	包年包月	预付费	提供基础防护带宽，预付费价格由保底防护峰值和购买时长确定。若升级保底防护，则在原有的基础上加收额外费用，且防护级别只可升不可降。
弹性防护峰值	按天按量计费	后付费	触发弹性防护后，按当天最高攻击峰值所对应的弹性防护峰值区间计费，账单次日生成。若未触发弹性防护，则不收取任何费用。支持升级、降级配置。
转发规则数	包年包月按个数计费	后付费	默认免费为每个高防 IP 提供60个转发规则数。当配置的规则数大于免费额度时，每增加10个按增加500元/月计算。单个 DDoS 高防 IP 实例最高可支持300个转发规则数。
业务带宽	包年包月按带宽计费	预付费	业务带宽限制是针对业务 IN 方向（高防回源流量）和业务 OUT 方向（高防出流量），业务带宽规格需要大于业务 IN 和业务 OUT 中最大流量值。如果实际业务带宽持续超过购买 DDoS 高防 IP 时所设置的业务带宽，可能会出现丢包现象，影响业务，建议及时调整业务带宽。

百 G 包年套餐

DDoS 防护能力	CC 防护能力	单价（元/年）
-----------	---------	---------

100Gbps	300,000QPS	328,000
200Gbps	500,000QPS	358,000
300Gbps	700,000QPS	368,000

说明：

- 百 G 包年套餐仅限中国内地（大陆）区域售卖。
- DDoS 防护能力为100Gbps的包年套餐，弹性防护峰值可以配置到300Gbps。弹性相关收费请参见 [弹性防护区间价格](#)。
- 支持对百 G 包年套餐进行按月续费，例如，100Gbps包年套餐32.8万元，续费2个月，则大致需要 5.47（32.8/12*2）万元。
- 建议选择最靠近业务源站的地域，可降低访问时延，提高访问速度。

保底防护

保底防护按月预付费，具体价格请参考如下表格：

DDoS 防护	CC 防护	大陆 BGP（元/月）	境外 BGP（元/月）
10Gbps	20,000QPS	—	20,000
20Gbps	40,000QPS	6,000	30,000
30Gbps	70,000QPS	16,600	47,000
40Gbps	100,000QPS	—	55,000
50Gbps	150,000QPS	25,600	67,000
60Gbps	200,000QPS	—	80,000
80Gbps	250,000QPS	—	90,000
100Gbps	300,000QPS	—	96,000

说明：

- Query Per Second（QPS），此处用于衡量 DDoS 防护 IP 实例每秒可防护的 CC 攻击请求数。
- 可提供 T 级防护能力，如有需要，请联系您的商务经理进行定制。
- 保底防护峰值为20Gbps/30Gbps/50Gbps的 DDoS 高防 IP，不支持升级为100Gbps及以上的保底防护规格，最大支持升级为50Gbps。

弹性防护

用户可根据实际业务防护需求自助开启弹性防护。

- 未开启弹性防护时，最高防护峰值为保底防护峰值且不会产生后付费。
- 开启弹性防护时，弹性防护峰值为实例的最高防护峰值。
- 未触发弹性防护时，不产生费用。
- 当触发弹性防护（攻击峰值超过保底防护峰值且在弹性防护范围内）时，取当天实际发生的最高攻击峰值所对应计费区间进行计费，账单次日生成。

弹性防护具体价格请参考如下表格：

DDoS 防护峰值	大陆 BGP（元/天）	境外 BGP（元/天）
10Gbps ≤ 攻击峰值 < 20Gbps	—	2,200
20Gbps ≤ 攻击峰值 < 30Gbps	3,500	2,800
30Gbps ≤ 攻击峰值 < 40Gbps	4,800	4,800
40Gbps ≤ 攻击峰值 < 50Gbps	5,700	5,700
50Gbps ≤ 攻击峰值 < 60Gbps	6,600	8,000
60Gbps ≤ 攻击峰值 < 70Gbps	7,500	12,000
70Gbps ≤ 攻击峰值 < 80Gbps	8,350	15,000
80Gbps ≤ 攻击峰值 < 90Gbps	9,200	17,000
90Gbps ≤ 攻击峰值 < 100Gbps	10,050	18,000
100Gbps ≤ 攻击峰值 < 120Gbps	11,750	20,000
120Gbps ≤ 攻击峰值 < 150Gbps	14,300	22,000
150Gbps ≤ 攻击峰值 < 200Gbps	18,550	27,000
200Gbps ≤ 攻击峰值 < 250Gbps	22,800	36,000
250Gbps ≤ 攻击峰值 < 300Gbps	26,800	40,000
300Gbps ≤ 攻击峰值 < 400Gbps	—	48,000

转发规则数

规则数	价格（元/月/10个）
-----	-------------

端口数（或防护域名数） ≤ 60	免费
端口数（或防护域名数） > 60	500

说明：

转发规则数指，单个高防 IP 实例，在非网站接入配置时支持添加的 TCP/UDP 端口数量，或网站接入配置时支持添加的 HTTP/HTTPS 域名数量。单个高防 IP 实例的转发规则数等于上述两种接入方式的转发规则数量之和。

业务带宽

业务带宽是指经过腾讯云高防机房完成清洗后转发回源站机房的正常业务流量所消耗的带宽。

目前支持的收费模式为包年包月预付费，对于大陆地区的非腾讯云上用户，购买保底套餐后默认赠送100Mbps转发带宽。具体价格请参考如下表格：

带宽	大陆价格（元/月）	境外价格（元/月）
50Mbps	—	4,500
100Mbps	0（默认赠送）	9,000
150Mbps	4500	13,500
200Mbps	9000	18,000
500Mbps	36000	45,000
1Gbps	81000	90,000
2Gbps	171,000	180,000

带宽与七层请求数对应关系请参考如下表格：

业务带宽	HTTP/HTTPS
50Mbps	5,000QPS
100Mbps	10,000QPS
150Mbps	15,000QPS
200Mbps	20,000QPS
500Mbps	50,000QPS
1Gbps	100,000QPS

2Gbps

200,000QPS

说明：

- 业务带宽限制是针对业务 IN 方向（高防回源流量）和业务 OUT 方向（高防出流量），业务带宽规格需要大于业务 IN 和业务 OUT 中最大流量值。如果实际业务带宽持续超过 [购买 DDoS 高防 IP](#) 时所设置的**转发业务带宽**，可能会出现丢包现象，影响业务，建议及时升级业务带宽。
- 此处 QPS 用于衡量非攻击状态下每秒的正常业务请求量。如果您的正常业务请求消耗过大超出所购买的规格，请及时 [调整 DDoS 高防 IP 实例规格](#) 避免因丢包造成业务影响。您可以参考上表中的带宽与七层请求数对应关系合理增加 DDoS 高防 IP 实例的业务带宽，提高 HTTP/HTTPS 的正常 QPS 规格。

其他规格

其他规格说明请参考如下表格：

规格名称	规格参数	说明
转发端口数	60个 – 300个/单个防护 IP	TCP/UDP 协议+ HTTP/HTTPS 协议转发规格条目总数，对于 TCP、UDP 协议，若使用相同的转发端口值，则需要配置两条。
支持域名数		
源站 IP 数	20个/单个实例	4层与7层源站服务器 IP 地址总数
每秒新建连接数	50000个/单个防护 IP	单个防护 IP 的每秒新建连接数
并发连接数	200000个/单个防护 IP	单个防护 IP 的并发连接数

说明：

以上规格仅针对线上售卖，如果此配置不足以满足您的业务需求，请联系 [腾讯云技术支持](#) 定制更大的规格。

计费示例

DDoS 高防 IP 使用组合计费方式，计费示例说明如下：

例如，用户在上海区域购买了一个 DDoS 高防 IP，规格是“20Gbps 保底防护峰值+50Gbps 弹性防护峰值”。

若当天发生 DDoS 攻击事件且最高攻击流量峰值为45Gbps，则45Gbps超过保底防护峰值范围且使用了弹性防护峰值，落入了 $40\text{Gbps} < \text{弹性峰值} \leq 50\text{Gbps}$ 计费区间，当天产生弹性费用5700元。

则用户需支付费用合计为11700元，其中包含当月的保底防护费用6000元，当天产生的弹性费用5700元。

购买指引

最近更新时间：2023-07-21 10:53:03

前提条件

在购买 DDoS 高防 IP 实例前，您需要完成 [注册腾讯云](#) 账号，并完成 [实名认证](#)。

操作步骤

1. 如需购买 DDoS 高防 IP，请进入 DDoS 高防 IP 购买页进行购买。

① 注意：

目前已不支持购买旧版 DDoS 高防 IP，如需购买 DDoS 高防 IP，可参见新版 DDoS 高防 IP [购买指引](#) 进行购买。

2. 根据实际需求配置如下参数。

① 说明：

以下参数仅针对旧版 DDoS 高防 IP 购买页进行说明。

- 地域：DDoS 高防 IP 提供代理转发方式，请选择靠近源站服务器位置的地域，减少访问时延。
- 保底防护峰值：按包年包月预付费。建议以历史攻击流量的平均值为参考，选择的保底防护峰值略高于平均值，以便足够防御大部分攻击行为。
- 弹性防护峰值：按实际防护量计费，每日结算。建议以历史最高攻击流量为参考，选择的弹性防护峰值略高于历史最高峰值，以便足够防御大流量攻击，避免超过防护峰值而引起的 IP 封堵。
- 业务带宽：业务带宽限制是针对业务 IN 方向（高防回源流量）和业务 OUT 方向（高防出流量），业务带宽规格需要大于业务 IN 和业务 OUT 中最大流量值。

① 说明：

如果实际业务带宽持续超过购买 DDoS 高防 IP 时所设置的业务带宽，可能会出现丢包现象，影响业务，建议及时调整业务带宽。

- 购买个数：设置需要购买的实例数量。
- 购买时长：设置需要购买的时长，将根据 IP 数量、保底防护峰值以及购买时长计算需要预付的费用。
- 自动续费：用户可自行勾选。开启自动续费后，在腾讯云账号余额充足情况下，服务到期后将按月自动续费，保障业务防护不中断。

购买类型

BGP高防

地域

华南地区

华东地区

华北地区

广州

上海

北京

保底防护峰值

20Gbps

30Gbps

50Gbps

100Gbps

CC防护峰值

40,000QPS

弹性防护峰值 ②

无

30Gbps

40Gbps

50Gbps

60Gbps

70Gbps

80Gbps

90Gbps

100Gbps

您当前还未开启弹性防护，建议开启弹性防护，可以帮助您更从容应对大流量DDoS攻击。具体可参考 [产品价格详情](#)

业务规格

100Mbps

150Mbps

200Mbps

500Mbps

1Gbps

2Gbps

业务带宽: 100Mbps
HTTP: 3000QPS
HTTPS: 3000QPS
当前业务带宽不够用或业务QPS需要更高时，请及时升级。具体可参考 [带宽价格](#)、[带宽与七层请求数对应关系](#)。如果以上规格无法满足业务需求，请联系腾讯云售前架构师定制。

购买时长

1个月

2个月

3个月

4个月

5个月

6个月

7个月

8个月

9个月

1年

2年

3年

自动续费

☐ 账户余额足够时，设备到期后按月自动续费

当前配置

购买类型

BGP高防

地域

广州

线路

BGP

保底防护峰值

20Gbps

CC防护峰值

40,000QPS

弹性防护

未开启

业务带宽

100Mbps

HTTP(QPS)

3000

HTTPS(QPS)

3000

购买时长

1个月

自动续费

否

总计费用

立即支付

3. 单击立即支付，完成支付流程。

更多信息

- DDoS 高防 IP 详细计费说明
- 计费相关常见问题

续费指引

最近更新时间：2023-07-21 09:44:39

为能继续享受正常的安全服务，用户可以在 DDoS 高防 IP 服务到期前为其手动续费，也可以设置到期自动续费。

续费提醒

DDoS 高防 IP 服务到期前7天，系统会向您推送服务即将到期、请及时续费等相关信息，信息通过站内信、短信及邮件的方式通知到腾讯云账号创建者以及所有协作者。具体详情请参考 [欠费说明](#)。

在 [购买 DDoS 高防 IP](#) 时，若已勾选并同意自动续费。在实例到期前，系统会向您发送提醒信息并自动生成续费订单，无需手动续费。

购买时长	☒ 1个月	☐ 2个月	☐ 3个月	☐ 4个月	☐ 5个月	☐ 6个月	☐ 7个月	☐ 8个月	☐ 9个月	☐ 1年	☐ 2年	☐ 3年
自动续费	☒ 账户余额足够时，设备到期后按月自动续费											

① 说明：

按月或按年开通的 DDoS 高防 IP 实例，其自动续费周期都为1个月。

续费方式

控制台续费

1. 登录 [DDoS 防护管理控制台](#)。
2. 选择 [DDoS 高防 IP](#) > [资产列表](#)，单击目标实例操作列中的[续费](#)。
3. 在续费页面选择[续费时长](#)，并完成相关支付流程。

续费管理中心续费

在 [续费管理页面](#) 提供实例的批量资源续费、设置自动续费、设置统一到期日以及取消不续费等功能，详见 [续费管理](#)。

调整规格费用说明

最近更新时间：2023-07-21 09:44:39

如果在使用 DDoS 高防 IP 过程中发现当前规格（如保底防护峰值、转发规则数或业务带宽等）已无法满足实际业务需求，您可以通过升级 DDoS 高防 IP 实例的规格来提升防护能力。

调整 DDoS 高防 IP 实例规格支持调高保底防护峰值，增加转发规则数（防护域名数或端口数）和调高业务带宽。

① 说明：

目前暂不支持降低已购买 DDoS 高防 IP 实例的规格。

升级 DDoS 高防 IP 实例规格，需要加收额外的升级费用。支付完成后，DDoS 高防 IP 实例规格升级即时生效。具体操作请参考 [调整规格](#)。

保底防护峰值

费用规则

- 调高保底防护峰值遵循按天补差价规则，计算方式：升配费用 = 按月升配差价 * 升配天数 / (365/12)。
- 按月升配差价 = 升级后服务的包月价格 - 当前服务的包月价格。
- 升配天数 = 资源到期时间 - 当前时间。
- 若调整的保底防护峰值等于或大于已设置的弹性防护峰值，则弹性防护不生效。
- 升配不影响资源到期时间。
- 升配可以使用代金券和平台赠送余额（赠送金）抵扣费用。

计费示例

① 说明：

以下示例仅供参考，费用请以实际扣费为准。实际单价详情请参见 [计费概述](#)。

2018年1月11日，购买一年20Gbps保底防护峰值的 DDoS 高防 IP 实例，每月6600元。在2018年12月18日，将该实例的保底防护峰值上调为30Gbps，每月12600元。

- 按月升配差价 = 12600 - 6600 = 6000元/月。
- 升配天数 = 13 + 11 = 24天。到期日期为2019年1月11日，12月18日到12月31日共计13天。
- 升配费用 = (12600 - 6600) * 24 / (365/12) = 4734.25元。

转发规则数

增加转发规则数所产生的额外费用计算规则：

- 防护域名数：每新增10个防护域名数按500元/月的单价与当前服务剩余时长计算额外费用。
- 端口数：每新增10个端口数按500元/月的单价与当前服务剩余时长计算额外费用。

业务带宽

调高业务带宽所产生的额外费用计算规则：每新增50Mbps业务带宽按4500/月的单价与当前服务剩余时长计算额外费用。

欠费说明

最近更新时间：2023-07-21 09:44:39

包年包月资源

到期提醒

对于包年包月的云资源服务，DDoS 高防 IP 系统会在到期前的7天内，向您推送“服务即将到期，请及时续费”等相关信息，信息通过站内信、短信、邮件或微信的方式，通知到腾讯云账号创建者以及所有协作者。

续费提醒

DDoS 高防 IP 实例在到期前7天内，系统会给腾讯云账号的创建者以及所有协作者发送续费提醒通知。

① 说明：

在账户余额充足的情况下，若用户已设置自动续费，系统在到期当日会自动续费。

回收机制

- 服务资源到期前7天，系统开始给用户发送续费提醒通知。
- 到期之日起24小时内，服务可以继续使用，同时系统会发送服务已到期提醒通知，若期间用户进行续费，则可以继续享受防护服务。
- 到期之日起24小时后，服务不可用，此 DDoS 高防 IP 实例将被回收至回收站中。用户可在 [控制台资源列表](#) 页面查看实例，并且仍然可以进行续费操作。
- DDoS 高防 IP 实例在回收站中最多保留7天，若7天内（包括第7天）仍未进行续费操作，则资源将在回收期后第8天被系统回收，配置数据将被清除且不可恢复。

按量计费资源

欠费提醒

系统会在每个整点对按量计费资源进行扣费。当您的账户被扣为负值时，系统将通过站内信、短信、邮件或微信的方式，通知到腾讯云账户的创建者以及所有协作者。

① 说明：

欠费提醒功能默认关闭。如您的账户开通了按量计费的资源，为了让您预知账户即将欠费，以预留一定的时间及时充值或备份数据，以保证云资源的正常使用，建议您前往腾讯云控制台 > 费用中心 > 主页 > [费用预警](#) 进行订阅。详细信息请参见 [余额预警指引](#)。

欠费处理

当您的账户余额被扣为负值时，DDoS 高防 IP 服务的弹性防护能力将会被关闭，但未到期的按月预付费保底防护能力和业务转发不受影响。在您的包年包月云资源有效期内，当您的账户余额充值为正值时，弹性防护能力将会自动恢复至欠费前所设置的弹性防护峰值。

退费说明

最近更新时间：2023-07-21 09:44:40

腾讯云 DDoS 高防 IP 服务不支持提前退订，不适用五天无理由退款。若您已购买 DDoS 高防 IP 实例，则不支持退款。

快速入门

接入非网站业务

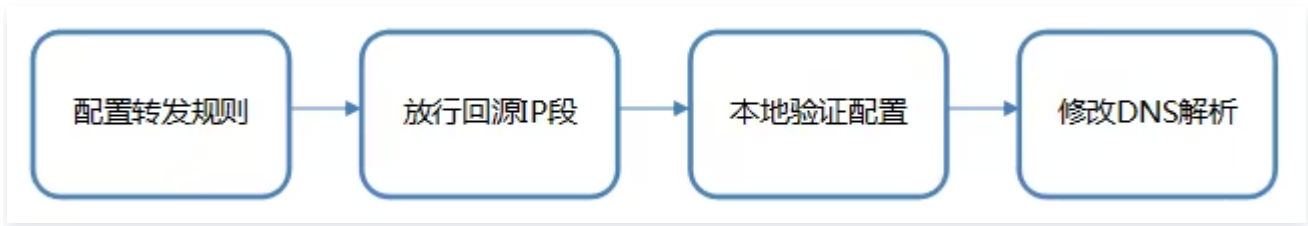
最近更新时间：2024-11-08 09:20:52

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 [云解析 DNS](#)。

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：
 - 2.1 单击**新建**。



2.2 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：

2.3 选择批量导入 > 导入转发规则。

2.4 在批量导入页面的规则输入框中，粘贴需要导入的规则。

① 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：

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：

1.1 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
```

1.2 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。

① 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。

① 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）。

① 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 [云解析 DNS 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
☐	...	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](#)。

← 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，否则将无法正常使用。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。如何解除锁定问题？查看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...	A	默认	1...	-	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

接入网站业务

最近更新时间：2024-11-08 09:20:52

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。

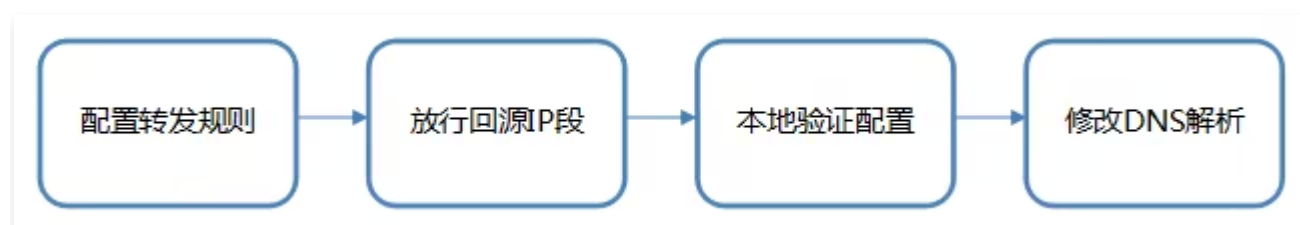
① 说明：

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 [云解析 DNS](#)。

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：
 - 2.1 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.

2.2 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

- 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：

2.1 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)

BGP

bgpip-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

https

转发端口

443

2.2 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

① 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：

1.1 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

1.2 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。

① 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。

① 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）。

① 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 [云解析 DNS 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**。

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，否则将无法正常使用。开始备案 [链接](#)
 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，解锁后即可正常使用。如何解除
 遇到问题？查看FAQ文档 [链接](#)

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	A	默认	1	-	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

操作指南

操作总览

最近更新时间：2023-07-21 09:44:40

您在使用 DDoS 高防 IP 时，可能碰到诸如配置 DDoS 高防 IP 实例、查看统计报表、查看操作日志以及设置安全事件通知等问题。本文将介绍使用 DDoS 高防 IP 的常用操作，供您参考。

实例管理

- [查看实例详情](#)
- [设置资源名称](#)
- [配置弹性防护](#)
- [调整 DDoS 高防 IP 实例规格](#)
- [解封防护 IP](#)

防护配置

- [配置业务场景](#)
- [配置清洗阈值与防护等级](#)
- [管理 DDoS 高级防护策略](#)
- [配置 CC 防护等级](#)
- [管理 CC 防护策略](#)
- [配置健康检查](#)
- [配置会话保持](#)

统计报表

[查看统计报表](#)

操作日志

[查看操作日志](#)

安全事件通知

[设置安全事件通知](#)

使用限制

最近更新时间：2025-03-17 15:00:32

防护对象建议

建议使用 DDoS 高防 IP 为腾讯云内外的业务 IP 或域名提供防护，支持对网站（七层）业务和非网站（四层）业务进行防护。

说明：

目前网站（七层）业务暂不支持境外区域接入，仅非网站（四层）支持境外区域接入。

转发能力限制

1个 DDoS 高防 IP 实例默认支持60条转发规则，最高可扩展至300条，非网站（四层）协议下每条规则支持20个源站 IP/域名，网站（七层）协议下则支持16个源站 IP/域名。

黑白名单配置限制

- DDoS 黑白 IP 名单之和最多支持添加100个 IP 地址。
- HTTP CC/HTTPS CC 黑白 IP 名单分别最多支持添加50个 IP 地址。
- HTTP CC/HTTPS CC URL 白名单最多支持添加50个 URL。

地域限制

目前已开放 DDoS 高防 IP 的地域包括：

- 中国内地（大陆）区域：华南地区（广州）、华东地区（上海）和华北地区（北京）。
- 境外区域：中国港澳台地区（香港、台湾）、亚太地区（新加坡、首尔、曼谷、日本）、美国东部（弗吉尼亚）、欧洲地区（法兰克福）。

DDoS 高防 IP 在不同地域提供的高防能力请参考如下表格：

地区	保底防护	弹性防护	最大防护能力
广州	20Gbps – 50Gbps	30Gbps – 100Gbps	100Gbps
北京	20Gbps – 50Gbps	30Gbps – 100Gbps	100Gbps
上海	20Gbps – 100Gbps	30Gbps – 300Gbps	300Gbps
境外区域	10Gbps – 100Gbps	30Gbps – 400Gbps	400Gbps

实例管理

查看实例详情

最近更新时间：2023-07-21 09:44:40

操作场景

您可以通过 [DDoS 防护管理控制台](#) 查看所购买的 DDoS 高防 IP 的基础信息（如实例保底防护峰值、运行状态）及实例的弹性防护配置。

操作步骤

本文将以查看广州地区高防 IP 实例 “bgpip-0000020n” 的详细信息为例进行详细说明。

1. 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**，在地区选择框中，单击 **华南地区（广州）**，并在下方列表中，找到并单击实例 ID 为 “bgpip-0000020n” 的高防 IP，查看实例信息。



2. 在弹出的页面查看如下信息：

bgpip-0000020n

基础信息 [编辑](#)

高防IP名称

IP

所在地区

华南地区(广州)

线路

BGP

转发目标

非腾讯云

保底防护峰值

20 Gbps [升级](#)

CC防护峰值

40000 QPS

当前状态

运行中

到期时间

2020-07-17 10:46:04 [续费](#)

标签

无 

回源IP段

弹性防护

当前状态

未开启 [开启](#)

想要提升防御可开启弹性防护，无攻击不计费

● 基础信息：

○ 高防 IP 名称

该 DDoS 高防 IP 实例的名称，用于辨识与管理 DDoS 高防 IP 实例。长度为1 – 20个字符，不限制字符类型。资源名称由用户根据实际业务需求自定义设置，具体操作请参考 [设置资源名称](#)。

○ IP

该 DDoS 高防 IP 实例所提供的高防 IP，作为源站的前置 IP 对外提供服务。

○ 所在区域

[购买 DDoS 高防 IP](#) 时选择的**地域**。

○ 转发目标

该 DDoS 高防 IP 实例所防护业务源站的位置。

○ DDoS 保底防护峰值

该 DDoS 高防 IP 实例的保底防护带宽能力，即 [购买](#) 时选择的**保底防护峰值**。若未开启弹性防护，则保底

防护峰值为高防服务实例的最高防护峰值。

- **CC 防护峰值**

该 DDoS 高防 IP 实例应对突发 CC 攻击的能力。

- **当前状态**

DDoS 高防 IP 实例当前的使用状态。状态包括运行中、清洗中以及封堵中等。

- **到期时间**

根据 [购买](#) 时选择的**购买时长**以及具体的提支付购买订单的具体时间计算所得，精确到秒级。腾讯云会在此时间前的第7天，通过站内信、短信及邮件的方式向腾讯云账号的创建者以及所有协作者推送服务即将到期并提醒及时续费的信息。

- **回源 IP 段**

根据当前 DDoS 高防 IP 的地域，显示该地域下的 DDoS 高防 IP 回源地址段信息，供用户查看了解。

- **弹性防护信息：**

- **当前状态**

表示弹性防护是否开启。若 [购买 DDoS 高防 IP 实例](#) 时未开启弹性防护，用户可在使用过程中自助开启，具体操作请参见 [配置弹性防护](#)。

- **弹性峰值**

表示当前 DDoS 高防 IP 实例的最大弹性防护带宽能力，用户可以根据自身业务需求，随时 [调整弹性防护峰值](#)。

① **注意：**

仅当开启弹性防护时，弹性峰值参数项才可见。

设置资源名称

最近更新时间：2023-07-21 09:44:41

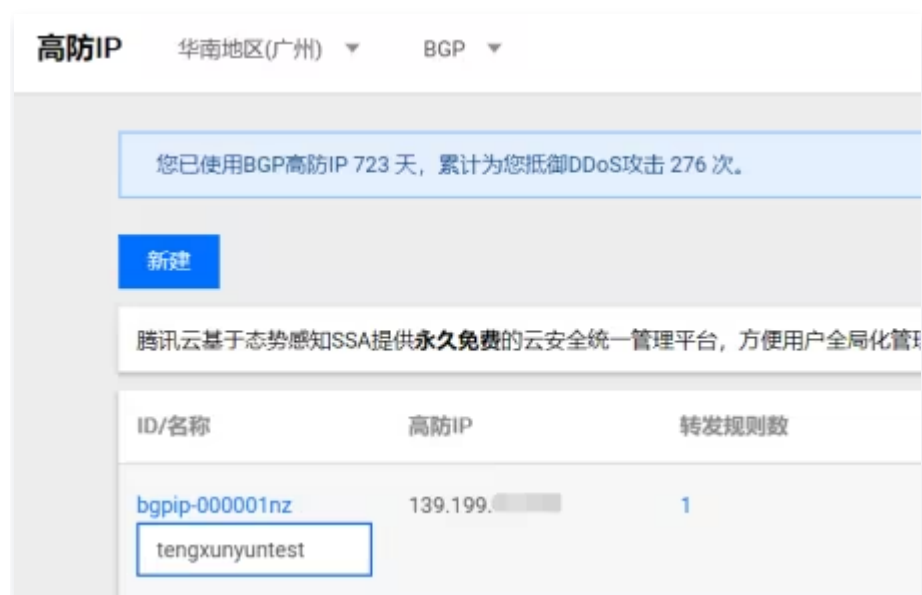
当使用多个 DDoS 高防 IP 实例时，可通过设置**资源名称**快速辨识与管理实例。

方式一

登录 [DDoS 防护管理控制台](#)，选择 **DDoS 高防 IP > 资产列表**，选择地域和线路，单击目标实例的**ID/名称**列的名称，输入名称即可。

① 说明：

名称长度为1 – 20个字符，不限制字符类型。



方式二

1. 登录 [DDoS 防护管理控制台](#)，选择 **DDoS 高防 IP > 资产列表**，在左上角选择地域。
2. 在下方列表中，单击目标实例的“ID/名称”列的实例 ID，在弹出页面的**基础信息**区域，单击**编辑**，输入或修改名称，并单击**确定**即可。

① 说明：

名称长度为1 – 20个字符，不限制字符类型。

基础信息

编辑

高防IP名称

IP

配置弹性防护

最近更新时间：2023-07-21 09:44:41

DDoS 高防 IP 实例启用弹性防护后，当攻击流量峰值超出保底防护峰值时，DDoS 高防 IP 会根据用户设置的弹性防护峰值继续进行防护。

若 [购买 DDoS 高防 IP 实例](#) 时，未开启弹性防护，用户可在使用过程中自助开启。当天未触发弹性防护，不产生额外费用。在触发弹性防护（攻击峰值超过保底防护峰值）时，取当天实际产生的最高攻击峰值所对应区间进行 [计费](#)，账单次日生成。用户可根据实际业务情况实时更改 DDoS 高防 IP 实例的弹性防护峰值。

开启弹性防护

① 说明：

若 [购买 DDoS 高防 IP 实例](#) 时未开启弹性防护，用户可在使用过程中开启，并以历史最高攻击流量为参考，选择略高于历史最高峰值的弹性防护峰值，以便足够防御大流量攻击，避免超过防护峰值而引起的 IP 封堵。

1. 登录 [DDoS 防护管理控制台](#)，选择 **DDoS 高防 IP > 资产列表**，在目标实例所在行，单击**开启弹性防护**。
2. 在**开启弹性防护**对话框中，选择需要的**弹性防护峰值**。

开启弹性防护

ID/名称

高防IP

弹性防护峰值

30Gbps40Gbps50Gbps60Gbps70Gbps80Gbps90Gbps100Gbps

在带宽峰值20Gbps的基础上，最高能够防御30Gbps的DDoS的攻击

费用说明

未触发弹性防护，不另收费用。
如果攻击发生当日流量带宽峰值超出20Gbps，会按照当日流量带宽峰值落入的计费区间进行计算，产生后付费账单。
计费区间如下：

弹性防护峰值(Gbps)	20~30	30~40	40~50	50~60	60~70	70~80	80~90	90~100
弹性防护费用(元/天)	3500	4800	5700	6600	7500	8350	9200	10050

确定提交

取消

3. 单击**确定提交**。

更改弹性防护峰值

1. 登录 [DDoS 防护管理控制台](#)，选择 **DDoS 高防 IP > 资产列表**，单击目的实例 ID，进入实例的基础信息界面。
2. 找到“弹性防护”部分，在“弹性峰值”右侧，单击**更改**。

服务包信息 [编辑](#)

高防IP名称	
IP	139
所在地区	华南地区(广州)
转发目标	非腾讯云
DDoS保底防护峰值	20 Gbps 升级
CC防护峰值	40000 QPS
当前状态	运行中
到期时间	2019-05-02 17:23:46 续费
弹性防护	
当前状态	已开启 关闭
弹性峰值	100Gbps 更改

3. 在**更改弹性防护**对话框中，选择合适的**弹性防护峰值**。

① 说明：

- 弹性防护峰值支持调升调降，不同地域支持的防护能力不同，弹性防护峰值的具体取值范围请参考 [产品概述](#)。
- 弹性防护峰值修改后立即生效。

更改弹性防护

ID/名称

高防IP

弹性防护峰值

30Gbps	40Gbps	50Gbps	60Gbps	70Gbps	80Gbps	90Gbps	100Gbps
--------	--------	--------	--------	--------	--------	--------	---------

在带宽峰值20Gbps的基础上，最高能够防御100Gbps的DDoS的攻击

费用说明

未触发弹性防护，不另收费用。

如果攻击发生当日流量带宽峰值超出20Gbps，会按照当日流量带宽峰值落入的计费区间进行计算，产生后付费账单。

计费区间如下：

弹性防护峰值(Gbps)	20~30	30~40	40~50	50~60	60~70	70~80	80~90	90~100
弹性防护费用(元/天)	3500	4800	5700	6600	7500	8350	9200	10050

确定提交

取消

4. 单击**确定提交**。

关闭弹性防护

说明：

关闭弹性防护后，最大防护峰值降为保底防护峰值，请确保是否满足实际需求再执行此操作。

1. 登录 [DDoS 防护管理控制台](#)，选择 **DDoS 高防 IP > 资产列表**，在目标实例所在行，单击**关闭弹性防护**。
2. 在**关闭弹性防护**对话框中，单击**确定提交**。

版权所有：腾讯云计算（北京）有限责任公司

第212 共285页

调整 DDoS 高防 IP 实例规格

最近更新时间：2023-07-21 09:44:41

操作场景

如果在使用 DDoS 高防 IP 过程中发现当前规格（如保底防护峰值和转发规则数或业务带宽等）已无法满足实际业务需求，您可以通过升级 DDoS 高防 IP 实例的规格来提升防护能力。

调整 DDoS 高防 IP 实例规格支持调高保底防护峰值，增加转发规则数（防护域名数或端口数）和调高业务带宽。

说明：

目前暂不支持降低已购买 DDoS 高防 IP 实例的规格。

升级 DDoS 高防 IP 实例规格，需要加收额外的费用。支付完成后，DDoS 高防 IP 实例规格升级即时生效。费用说明请参考 [调整规格费用说明](#)。

操作步骤

1. 登录 [DDoS 防护管理控制台](#)。
2. 选择 **DDoS 高防 IP > 资产列表**。
3. 单击目标 DDoS 高防 IP 实例所在行的**升级**。

ID/名称	高防IP	转发规则数	转发目标	超峰次数 🔍	运行状态	到期时间	自动续费	操作
		2	非腾讯云	0	运行中	2020-07-17 10:46:04	☐	升级 续费 防护配置 查看报表 关闭弹性防护

4. 根据实际需求设置**升级保底防护**、**升级业务带宽**以及**升级转发规则数**。

升级

ID/名称

bgpip-000001lb /

高防IP

212.

当前保底防护峰值

20 Gbps

过期时间

2019-09-12 09:55:55

升级保底防护

20 Gbps

30 Gbps

50 Gbps

100 Gbps

cc防护峰值：40,000QPS

升级业务带宽

100Mb

150Mb

200Mb

500Mb

1000Mb

2Gb

升级转发规则数

60

70

80

90

100

150

200

250

300

5. 单击**立即升级**，进入**核对信息**页面。

6. 确认无误后，根据实际情况选择是否使用代金券，单击**确认购买**。

7. 完成支付后，返回 DDoS 高防 IP 资产列表即可查看规格调整已即刻生效。

解封防护 IP

最近更新时间：2023-07-27 11:17:13

DDoS 高防 IP 对进入封堵状态的防护 IP 提供解封的功能，您可以登录 [DDoS 防护管理控制台](#) 进行自助解封操作。

自助解封次数

使用 DDoS 高防 IP 的用户每天将拥有三次自助解封机会，当天超过三次后将无法进行解封操作。系统将在每天零点时重置自助解封次数，当天未使用的解封次数不会累计到次日。

说明：

- 由于解封涉及腾讯云 DDoS 防护系统的风控管理策略，解封可能失败（解封失败不会扣减您的剩余解封次数），请您耐心等待一段时间后再尝试。
- 在执行解封操作前，建议您先查看预计解封时间，预计解封时间受到部分因素影响，可能会推后。如果您可以接受预计时间，则无需手动操作。
- 当天自助解封配额为0时，建议提升保底防护能力或弹性防护能力，以便足够防御大流量攻击，避免被持续封堵。

自助解封操作

登录 [DDoS 防护管理控制台](#)，选择自助解封>解封操作，找到状态为自动解封中的防护 IP，单击操作列中的解封。在解除封堵对话框中，单击确定。

- 如果解封失败，您会收到解封失败提示信息，请您耐心等待一段时间后再尝试。
- 如果收到解封成功提示信息，则表示封堵状态已成功解除，您可以刷新页面确认该防护 IP 是否已恢复运行中状态。

解封操作				
总配额数		当前已使用		当前未使用
3 次		0 次		3 次
IP	封堵时间	预计解封时间	状态	操作
119.29.245.153	2018-11-07 20:31:37	2018-11-07 22:31:37	自动解封中	解封

解封操作记录

登录 [DDoS 防护管理控制台](#)，选择自助解封>解封操作记录，根据时间范围筛选，可查看所有解封操作记录，包括自动解封、手工自助解封等操作记录。

解封操作记录

2018-08-09 20:38:41 至 2018-11-07 20:38:41 

IP	封堵时间	实际解封时间	解封操作类型
123.206. 	2018-10-18 15:49:52	2018-10-18 16:05:09	自助解封
123.206. 	2018-10-17 16:21:40	2018-10-17 16:52:02	自动解封
123.206. 	2018-10-17 16:16:50	2018-10-17 16:47:16	自动解封
193.112. 	2018-09-14 17:37:45	2018-09-14 18:17:26	自助解封

防护配置

配置业务场景

最近更新时间：2023-07-21 09:44:41

应用场景

DDoS 高防 IP 支持自定义 DDoS 高级防护策略，用户可以根据业务特点或攻击行为针对性地设置防护策略。通常每个 DDoS 高防 IP 实例最多绑定一个 DDoS 高级防护策略。当用户的账号下拥有多个高防 IP 实例时，最多拥有 5 个 DDoS 高级防护策略可供选择。

为满足实际业务需要或应对不断变化的攻击手法，用户可能需要不断优化策略配置。为简化 DDoS 精细化防护管理，DDoS 高防 IP 提供业务场景设置功能，通过创建业务应用场景，后台收集、识别并自动生成高级防护策略，实现灵活的配置或维护策略。

创建业务场景

方法一

若用户所购 DDoS 高防 IP 实例未配置业务场景，登录 [DDoS 防护管理控制台](#)，在左侧导航中选择 **DDoS 高防 IP > 防护配置**，会弹出如下图所示提示信息，单击**去创建**，进行业务场景创建。



说明：
最多支持创建5个业务场景。

方法二

1. 登录 [DDoS 防护管理控制台](#)，在左侧导航中选择 **DDoS 高防 IP > 防护配置**，在配置页面中，选择 **DDoS 高级防护策略 > 创建业务场景**。

防护配置

防护策略

CC攻击防护

DDoS高级防护策略

创建业务场景

业务名称

高级策略名称

test

test_policy_82

2. 在创建业务场景页面，根据实际业务特点，输入以下参数，单击**确定**，完成1个业务场景的设置。

创建业务场景

业务名称(必填)

平台开发

☐ PC客户端

☐ 移动端

☐ 电视端

☐ 主机

细分品类

无

基础信息

是否有海外客户?

☐ 是

☐ 否

☒ 暂无法确认

是否会主动对外发起TCP请求?

☐ 是

☐ 否

☒ 暂无法确认

是否会主动向外发起UDP业务请求(如DNS请求, NTP请求等)?

☐ 是

☐ 否

☒ 暂无法确认

其他信息 收起-

UDP载荷是否有固定特征?

☐ 是

☒ 否

TCP载荷是否存在固定特征?

☐ 是

☒ 否

是否存在Web API业务? (使用,分隔)

☐ 是

☒ 否

确定

取消

- **业务名称**：必填项，输入业务名称，长度为1 – 32个字符，不限制字符类型。
- **平台开发**：勾选平台开发对应的类型。可供选择的有 PC 客户端、移动端、电视端和主机。

- **细分品类：**选择业务所属类型。可供选择的有游戏、应用、网站或其他类型。
- **基础信息：**
 - **是否有海外客户？**
勾选是、否或暂无法确认。对应生成策略的配置项为关闭或开启**拒绝海外流量**。
 - **是否会主动对外发起 TCP 请求？**
勾选是、否或暂无法确认。选择是时，需要填写主动对外发起 TCP 请求的端口。存在多个请求业务端口时，全部填入并用英文“,”分隔。
 - **是否会主动向外发起 UDP 业务请求（如 DNS 请求，NTP 请求等）？**
勾选是、否或暂无法确认。选择是时，需要填写主动对外发起 UDP 业务请求的端口。存在多个请求业务端口时，全部填入并用英文“,”分隔。
- **其他信息：**（单击**展开+**即可对参数进行选择）
 - **UDP 载荷是否有固定特征？**
勾选是或否。默认否，当选择是时，需要填写 UDP 载荷特征内容。
 - **TCP 载荷是否存在固定特征？**
勾选是或否。默认否，当选择是时，需要填写 TCP 载荷特征内容。
 - **是否存在 Web API 业务？（使用英文“,”分隔）**
勾选是或否。默认否，当选择是时，需要填写 API 业务 URL。存在多个 API 业务 URL 时，全部填入并用英文“,”分隔。

3. 后台对用户创建的业务场景进行分析后，自动生成1条以“业务场景名称_policy_序号”（如“test_policy_1”）命名的高级防护策略，用户再根据实际特殊业务防护需求，自主配置或调整该条防护策略。

① 说明：

- 在用户只拥有一个 DDoS 高防 IP 实例（资源）情况下，若只创建一个业务场景，则自动将对应生成的高级防护策略绑定到当前实例（资源）中。
- 当对业务场景信息修改后，对应生成的高级防护策略会自动同步相关配置项信息。若对该条高级防护策略进行调整，则不会同步到对应的业务场景信息。
- 当以“业务场景名称_policy_序号”的高级防护策略绑定了一个或多个实例（资源）时，若对其中一个实例（资源）的转发规则参数（如下列参数）进行修改后，
 - 则对应高级防护策略中对应的配置项信息会自动同步。
 - （四层）非网站业务：TCP/UDP 协议，转发端口范围。
 - （七层）网站业务：HTTP/HTTPS 协议，转发端口默认80/443。

修改和删除业务场景

1. 登录 [DDoS 防护管理控制台](#)，在左侧导航中选择**DDoS 高防 IP>防护配置**。
2. 单击**DDoS 高级防护策略**，找到目的业务场景，单击**配置或删除**，进行修改或者删除。

① 注意：

当对目的业务场景进行删除操作，则对应的高级防护策略也将删除。

创建业务场景			
业务名称	高级策略名称	创建时间	操作
test	test_policy_82	2019-07-01 19:42:12	配置 删除

若想了解更多信息，请参见 [管理 DDoS 高级防护策略](#)。

配置清洗阈值与防护等级

最近更新时间：2023-07-21 10:53:03

应用场景

DDoS 高防 IP 服务提供防护策略调整功能，针对 DDoS 攻击提供三种防护等级供您选择，各个防护等级的具体防护操作如下：

① 注意：

如果业务需要使用 UDP，建议联系 [腾讯云技术支持](#) 进行策略定制，以免严格模式影响业务。

默认情况下，您所购买的 DDoS 高防 IP 实例采用正常防护等级，您可以根据实际业务情况自由调整 DDoS 防护等级。同时，您还可以自定义设置清洗阈值，当攻击流量超过设置的阈值时，将启动清洗策略。

防护等级	防护操作	描述
宽松	- 过滤明确攻击特征的 SYN、ACK 数据包。 - 过滤不符合协议规范的 TCP、UDP、ICMP 数据包。 - 过滤具有明确攻击特征的 UDP 数据包。	清洗策略相对宽松，仅对具有明确攻击特征的攻击包进行防护。建议在怀疑有误杀时启用，遇到复杂攻击时可能会有攻击透传。
正常	- 过滤明确攻击特征的 SYN、ACK 数据包。 - 过滤不符合协议规范的 TCP、UDP、ICMP 数据包。 - 过滤具有明确攻击特征的 UDP 数据包。 - 过滤常见基于 UDP 的攻击数据包。 - 对部分访问源 IP 进行主动验证。	清洗策略适配绝大多数业务，可有效防护常见攻击。默认为正常模式。
严格	- 过滤明确攻击特征的 SYN、ACK 数据包。 - 过滤不符合协议规范的 TCP、UDP、ICMP 数据包。 - 过滤具有明确攻击特征的 UDP 数据包。 - 过滤常见基于 UDP 的攻击数据包。 - 对部分访问源 IP 进行主动验证。 - 过滤 ICMP 攻击包。	清洗策略相对严格，建议在正常模式出现攻击透传时使用。

- 过滤常见的 UDP 攻击数据包。
- UDP 数据包严格检查。

配置示例

下面以配置华南地区（广州）的实例“bgpip-000002ai”为例，进行配置说明：

1. 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**，在地区选择框中，单击**华南地区（广州）**。
2. 在下方实例列表中，找到目标高防 IP 实例 ID 为“bgpip-000002ai”的高防 IP 实例，在右侧操作项中，单击**防护配置**，进行配置。

ID/名称	高防IP	转发规则数	转发目标	超峰次数	运行状态	到期时间	自动续费	操作
bgpip-000002ai		3			运行中	2020-12-12 10:44:33		升级 续费 防护配置 查看报表 开启弹性防护

3. 在弹出的 DDoS 防护配置的页面中，开启**防护状态**，进行清洗阈值、防护等级的设置。

① 说明：

仅当防护状态为 状态时，配置项才可见。若手动将防护状态关闭，则配置项隐藏且配置不生效。重新开启后，配置项可见且保持原有的配置数据。

DDoS防护配置

防护状态

清洗阈值 ①

默认

防护等级 ①

宽松 正常 **严格**

业务场景

无

高级策略

无

DDoS攻击告警阈值

未设置

TCP业务AI增强防护

配置参数说明：

• 防护状态

默认开启，您可根据实际业务需求开启或关闭防护。关闭防护时，可进行关闭时长的设置，目前只能临时关闭防护1 - 6小时，超过所设置的时长或当攻击流量超过100wpps或2Gbps时，DDoS 高防包将自动开启防护。

• 清洗阈值

- 清洗阈值是高防产品启动清洗动作的阈值。当流量小于阈值时，即使检测到攻击也不会进行清洗操作。
- 默认在开启“防护状态”的情况下，业务刚接入的 DDoS 高防IP实例的清洗阈值采用默认值，并随着接入业务流量的变化规律，系统自动学习形成一个基线值。您可以根据实际业务情况自由设置清洗阈值。

① 说明：

若明确该清洗阈值，可进行自定义设置。若无法明确该清洗阈值，DDoS 防护系统将根据 AI 算法自动学习并生成一套专属的默认阈值。

- **防护等级**

默认在开启“防护状态”的情况下，业务刚接入的 DDoS 高防 IP 实例采用正常防护等级，您可以根据实际业务防护需求自由调整 DDoS 防护等级。

- **其他配置项**

- **业务场景**

您可以根据实际业务需求，从已创建的业务场景中选择一个匹配的业务场景，且支持修改。当选择某一个业务场景后，对应的“高级策略”会自动匹配该业务场景生成的策略。详情请参见 [配置业务场景](#)，进行业务场景创建。

- **高级策略**

您可根据业务防护特性，从已创建的高级策略中选择一个匹配的高级策略，且支持修改。详情请参见 [管理 DDoS 高级防护策略](#)，进行高级防护策略创建。

- **DDoS 攻击告警阈值**

DDoS 攻击告警阈值配置功能。若检测的指标超过您设定的阈值，将触发告警，并向您推送攻击告警信息。详情请参见 [配置攻击告警阈值](#)，进行告警指标设置。

- **TCP 业务 AI 增强防护**

针对四层 TCP 业务，DDoS 高防 IP 提供 TCP 业务 AI 增强防护功能。功能开启后，通过 AI 模型日常业务特征的自学习，能够自动识别业务流量与攻击流量，有效防护线上的四层 CC 攻击。

① 注意：

目前 TCP 业务 AI 增强防护功能仅对白名单开放。

管理 DDoS 高级防护策略

最近更新时间：2023-07-27 11:17:13

DDoS 高防 IP 提供面向 DDoS 攻击的高级防护策略功能，用户可针对自身业务防护需求对 DDoS 防护策略进行调整和优化。通过黑白名单、禁用协议、端口禁用（丢弃）或放行、报文特征过滤策略、连接耗尽防护、水印防护等功能，为业务提供针对性防护。

配置项简介

配置项	功能简介	生效时间
黑白名单	基于 IP 地址级别的防护。 - 白名单中的 IP，访问时将被直接放行，不经过任何防护策略过滤。 - 黑名单中的 IP，访问时将会被直接阻断。	当被防护的 IP 处于被攻击状态时生效。
禁用协议	可禁用业务不使用的协议。 当检测到攻击行为时，DDoS 高防集群会清洗掉该协议的流量。	当被防护的 IP 处于被攻击状态时生效。
端口禁用（丢弃）或放行	可禁用或放行来自指定类型端口的流量。	当检测到攻击行为时，DDoS 高防集群会清洗掉（或放行）该指定端口或指定端口范围的流量。
报文过滤特征	可以针对业务报文特征或攻击报文特征，将协议、端口范围、包长范围、是否检测载荷、偏移量、检查深度、是否包括特征字符串等条件进行组合，设定策略动作。 当检测到报文匹配到策略条件时，可以执行直接转发、丢弃、拉黑源 IP 或断开连接等操作。	当被防护的 IP 处于被攻击状态时生效。
限速	基于目的IP的防护，对访问协议进行限速控制。	当被防护的 IP 处于被攻击状态时生效。
拒绝海外流量	可拒绝来自中国（大陆地区及港澳台）以外的 TCP 流量请求。	当被防护的 IP 处于被攻击状态时生效。
连接耗尽防护	基于 IP 地址的防护，对于接入高防 IP 的非网站业务的 IP 的连接速度、包长度等参数进行限制，实现缓解小流量的连接型攻击的防护功能。	当被防护的 IP 处于被攻击状态时生效。

异常连接检测	当一个源 IP 接收到的一个 TCP 连接符合所配置的参数特征时，将判断为异常连接，同时当该源 IP 所接收到的异常连接数超过所设置的最大异常连接数时，会被加入黑名单一定时间，禁止被访问。	当被防护的 IP 处于被攻击状态时生效。
水印防护	支持 UDP 和 TCP 报文，在配置的端口范围内，其载荷进行水印检测和剥离。通过接入水印防护，高效全面防护 4 层 CC 攻击，如模拟业务报文攻击和重放攻击等。 业务端和腾讯云 DDoS 安全防护系统端共享水印算法和密钥。 - 客户端每个发出的报文都嵌入了水印特征，而攻击报文却无水印特征。 - DDoS 安全防护系统将甄别出攻击报文并将其丢弃。	当被防护的 IP 处于被攻击状态时生效。

添加新策略

① 注意：

高级安全防护策略功能具有一定专业性，建议有相关经验的用户在阅读以下操作指南后根据实际情况进行配置。

登录 [DDoS 防护管理控制台](#)，选择 **DDoS 高防 IP > 防护配置**。在 **DDoS 高级防护策略**页签，单击**添加新策略**。根据实际业务需求设置以下参数，单击**确定**。

策略名称

黑白名单

添加

请输入要查询的IP

策略	地址	操作
记录为空		

共0项

每页显示行 10

1/1

高级安全策略

禁用协议

☐ ICMP ☐ TCP ☐ UDP ☐ 其他协议

端口号

协议	端口类型	端口号	动作	操作
TCP	目的端口		丢弃	删除

增加

报文过滤特征

协议	开始源	结束源	开始目	结束目	最小包长	最大包长	检测载荷	正则表	偏移量	检查深度	是否包括	字符串	策略	操作
暂无记录，点击添加														

限速

协议	限速阈值	操作
暂无记录，点击添加		

● 策略名称

输入策略名称，长度为1 – 32个字符，不限制字符类型。

● 黑白名单

- 若需设置黑名单：单击添加，选择黑名单，填写需要拦截的 IP，存在多个 IP 时可全部填入并用回车分隔多个 IP，单击确定。
- 若需设置白名单：单击添加，选择白名单，填写需要放行的 IP，存在多个 IP 时可全部填入并用回车分隔多个 IP，单击确定。

① 说明：

黑白 IP 名单之和最多支持添加100个 IP，批量添加的 IP 数不允许超过当前配额。



● 禁用协议

选择需要禁用的协议，支持可选的禁用协议有 ICMP、TCP、UDP 和其他协议，这里的其他协议指除了 ICMP、TCP、UDP 以外的协议。

● 端口号

选择协议和端口类型，然后填写对应的端口，根据您的业务选择丢弃或放行动作。若需要对连续的端口范围进行配置，您可以按照“起始端口-结束端口”进行配置。例如要选择只允许30到80的端口通过，其余的直接丢弃，则应配置如下：

端口号				
协议	端口类型	端口号	动作	操作
TCP	目的端口	30-80	放行	删除
TCP	目的端口	1-65535	丢弃	删除

● 报文过滤特征

支持将协议、端口范围、包长范围、是否检测载荷、偏移量、检查深度、是否包括特征字符串等条件进行组合，设定策略动作且即刻生效。

① 说明：

- 偏移量：表示报文内容中开始匹配的特征的位置。
- 检查深度：配合偏移量使用，表示从偏移量设定的位置开始向后匹配的报文内容长度。
- 策略：
 - “丢弃报文”表示丢弃匹配该报文过滤特征的数据包。
 - “丢弃且拉黑源 IP”表示丢弃匹配该报文过滤特征的数据包并将源 IP 临时拉黑一段时间。
 - “丢弃且断开连接”表示丢弃匹配该报文过滤特征的数据包并断开 TCP 连接。
 - “丢弃，断开连接且拉黑源 IP”表示丢弃匹配该报文过滤特征的数据包，同时断开 TCP 连接并将源 IP 临时拉黑一段时间。

- “直接转发”表示直接转发匹配该报文过滤特征的数据包。

● 限速

单击**添加**，选择需要限速的协议，设置限速阈值。支持限速的可选协议有 ICMP、TCP、UDP 和其他协议，这里的其他协议指除了 ICMP、TCP、UDP 以外的协议。

● 拒绝海外流量

勾选**开启**或**关闭**。DDoS 高防 IP 的防护引擎内置海外 IP 库，开启拒绝海外流量后将基于该 IP 库对来源进行判断并执行阻断。勾选**开启**时，需处于被攻击状态才生效。勾选**关闭**时即刻生效。

连接耗尽防护

空连接防护 ①

☒ 关闭 ☐ 开启

源新建连接限速

☒ 关闭 ☐ 开启

源并发连接限制

☒ 关闭 ☐ 开启

目的新建连接限速

☒ 关闭 ☐ 开启

目的并发连接数限制

☒ 关闭 ☐ 开启

异常连接检测 ①

☒ 关闭 ☐ 开启

源IP最大异常连接数

☒ 关闭 ☐ 开启

水印防护

TCP防护端口	UDP防护端口	UDP水印剥离	策略开关	操作
点击开启				

确定

取消

● 连接耗尽防护

- **空连接防护**：勾选**开启**或**关闭**。勾选**开启**时，需处于被攻击状态才生效。由于基于 TCP 代理原理实现，对于业务的首次访问体验可能会有影响。
- **源新建连接限速**：勾选**开启**或**关闭**。勾选**开启**时，设置抑制速率（单位：个/秒），可填范围 0-∞。表示单一源IP每秒新建连接速率，超过限制的新建连接将被丢弃。
- **源并发连接限制**：勾选**开启**或**关闭**。勾选**开启**时，设置抑制数（单位：个），可填范围 0-∞。表示单一源IP并发连接数，超过限制的并发连接将被丢弃。
- **目的新建连接限速**：勾选**开启**或**关闭**。勾选**开启**时，设置抑制速率（单位：个/秒），可填范围 0-∞。表示目的IP每秒最大新建连接速率，超过限制的新建连接将被丢弃。由于防护设备为集群化部署，新建连接限速存在一定误差。
- **目的并发连接限制**：勾选**开启**或**关闭**。勾选**开启**时，设置抑制数（单位：个），可填范围 0-∞。表示目的IP 最大并发连接数，超过限制的并发连接将被丢弃。由于防护设备为集群化部署，并发连接限速存在一定误差。

● 异常连接检测

- **源IP最大异常连接数**：单击**开启**，填写源 IP 最大异常连接数量，可填范围 0-∞（单位：个）。表示当一个源 IP 符合异常连接行为识别的连接数，超过所指定阈值时，会被认为是异常攻击源，在一定时间内被限制

访问。

说明：

只有开启源 IP 最大异常连接数，以下参数才能进行配置。

- **Syn 报文占比检测：**勾选开启或关闭。勾选开启时，设置 Syn 报文占比值，可填范围 0-100。表示当一个 TCP 连接中的 Syn 报文数与 Ack 报文数的比例超过所配置阈值时，会被识别为一个异常连接。
- **Syn 报文数检测：**勾选开启或关闭。勾选开启时，设置最大报文数，可填范围 0-65535。表示当一个 TCP 连接中的 Syn 报文数超过所配置最大报文数时，会被识别为异常连接。
- **连接超时检测：**勾选开启或关闭。勾选开启时，设置检测周期（单位：秒），可填范围 0-65535。表示一个 TCP 连接创建后在所设置的时间内没有任何报文传输则判断为异常连接。
- **异常空连接检测：**勾选开启或关闭。表示一个 TCP 连接创建后没有任何带有载荷的报文传输则判断为异常连接。

● **水印防护**

单击**开启**进行水印防护配置。填写指定的 TCP 协议防护端口和 UDP 协议防护端口，单击**确定**水印防护功能即刻开启。添加 DDoS 高级防护策略后，自动产生一条密钥信息，需要完成线下客户端接入水印配置。

水印创建

TCP协议防护端口

开始端口号	结束端口号	操作
暂无记录，点击 添加		

TCP防护端口最多可以配置5个端口段；不同端口段不可以互相重合；起止端口号相同则认为是一个端口；TCP或UDP协议端口段需要至少配置一条。

UDP协议防护端口

开始端口号	结束端口号	操作
暂无记录，点击 添加		

UDP防护端口最多可以配置5个端口段；不同端口段不可以互相重合；起止端口号相同则认为是一个端口；TCP或UDP协议端口段需要至少配置一条。

自动剥离UDP报文水印

☒ 关闭 ☐ 开启

数据报文经过安全防护系统后，自动剥离UDP报文中的水印，再前传到源站。

偏移量

0

指定水印标签在UDP报文中的偏移量，可填范围 0-99

确定

取消

• TCP 协议防护端口、UDP 协议防护端口

TCP/UDP 防护端口最多可以配置5个端口段；不同端口段不可以互相重合；起止端口号相同则认为是一个端口；TCP 或 UDP协议端口段中需要至少配置一条。

① 说明：

只有在配置 UDP 协议端口段时，才可进行 UDP 水印剥离，同时可以指定水印标签在 UDP 报文中的偏移量。

• UDP 水印剥离

勾选 **自动剥离 UDP 报文水印**。数据报文经过 DDoS 高防系统后，自动剥离 UDP 报文中的水印，再前传到源站。

① 说明：

若不需要 DDoS 安全防护系统剥离 UDP 协议水印，则客户端仍需要做剥离水印的改造。

• 偏移量

指定水印标签在 UDP 报文中的偏移量，默认为0，可填范围 0-99。偏移量只有在 UDP 水印剥离开启后才起作用。

绑定与解绑资源

登录 [DDoS 防护管理控制台](#)，选择DDoS 高防 IP>防护配置。在DDoS 高级防护策略页签，单击目标策略所在行的绑定资源。

- 绑定资源：在弹出的**绑定资源**对话框中，根据实际业务需求勾选一个或多个资源，单击**确定**。
- 解绑资源：在弹出的**绑定资源**对话框中，根据实际业务需求单击**已选择区域**中已选资源右侧的 ，单击**确定**。

添加新策略			
策略名称	绑定资源数量	创建时间	操作
	0	2019-04-15 09:41:40	配置 删除 绑定资源 水印密钥配置 水印客户端接入文件下载
	0	2019-04-15 15:18:32	配置 删除 绑定资源 水印密钥配置 水印客户端接入文件下载

客户端接入水印

登录 [DDoS 防护管理控制台](#)，选择 DDoS 高防 IP > 防护配置。在DDoS 高级防护策略页签，单击目标策略所在行的**水印客户端文件下载**，线下完成客户端的接入。

添加、删除或停用/启用水印密钥

登录 [DDoS 防护管理控制台](#)，选择 DDoS 高防 IP > 防护配置。在 DDoS 高级防护策略页签，单击目标策略所在行的**水印密钥配置**。

- **添加密钥**：在弹出的**密钥信息**对话框中，单击**添加密钥**即刻生成新密钥。
- **停用/启用密钥**：支持对密钥进行停用或启用操作。在弹出的**密钥信息**对话框中，单击目的密钥所在行的**停用**；如需重新开启则单击**启用**即可。
- **删除密钥**：只能对已停用的密钥进行删除。在弹出的**密钥信息**对话框中，单击目的密钥所在行的**删除**即可。

① 说明：

最多可存在2个密钥，如果需要添加新密钥，请先删掉其中一个旧密钥；当仅有一个密钥生效时，不可将其停用或删除。

密钥信息

×

每个业务最多可以使用2个密钥，如果您需要添加新密钥，请先删除旧密钥；当仅有一个生效密钥时，不可停用和删除。

密钥	状态	生成时间	操作
	已停用	2019-04-18 18:57:45	复制 启用 删除
	已开启	2019-04-22 17:04:13	复制 停用

添加密钥

取消

配置策略

登录 [DDoS 防护管理控制台](#)，选择 **DDoS 高防 IP > 防护配置**。在 **DDoS 高级防护策略**页签，单击目标策略所在行的**配置**。根据实际业务需求更新以下参数，单击**确定保存修改**。

① 说明：

当目的策略是以“业务场景名称policy序号”形式命名的，则不能对策略名称进行修改。

- 策略名称
- 黑白名单
- 禁用协议
- 端口号
- 报文过滤特征
- 拒绝海外流量
- 连接耗尽防护
- 异常连接检测
- 水印防护

删除策略

说明：

- 未绑定资源的策略可直接删除，已绑定资源的策略需要先将所有资源解绑再执行删除操作。
- 若已开启 UDP 水印剥离开关，则删除策略会同步关闭 UDP 水印剥离开关，请确认业务客户端和服务端已完成相应的配置或者变更后，再执行删除操作。
- 策略删除后不可恢复，请谨慎操作。
- 不能对根据用户创建的业务场景自动生成的高级防护策略进行删除操作。

登录 [DDoS 防护管理控制台](#)，选择DDoS 高防 IP>防护配置。在DDoS 高级防护策略页签，单击目标策略所在行的删除。在弹出的对话框中，单击确定。



配置 CC 防护等级

最近更新时间：2023-07-21 09:44:41

防护说明

为了提升防护效果，减少防护出现误拦截风险，DDoS 高防 IP 服务针对 CC 攻击设计了3种防护等级供用户选择，默认提供正常等级。

- **宽松等级**：当受防护网站无明显流量异常时，可以采用此等级。同时该等级对受防护网站的所有请求都进行较为宽松的人机识别算法校验，即针对每个访问者进行验证，只有通过认证后访问者才允许访问网站。由于此等级下的 CC 防护策略较为宽松，可能会存在少部分异常请求透传的风险。
- **正常等级**：此等级为默认的 CC 防护等级，当发现受防护网站遭受 CC 攻击时，建议采用此等级。相对于宽松等级，正常等级的 CC 防护可以覆盖大部分攻击场景，能够防御大部分的 CC 攻击。同时，该等级会对受防护网站的所有请求，都进行人机识别算法校验，即针对每个访问者进行验证，只有通过认证后访问者才允许访问网站。
- **严格等级**：此等级下 CC 攻击防护策略较为严格，能防护更为复杂的 CC 攻击。同时，该等级会对所有访问请求实行严格的人机识别算法验证，即针对每个访问者都将进行验证，只有通过认证后才允许访问网站。由于此模式验证机制较为严格，部分正常请求存在被误拦截的风险。

① 注意：

- 上述三种 CC 防护等级所采用的防护算法只适用于网页或 H5 页面类的站点。
- 如果被访问网站的业务是 API 或原生 App 应用，由于该类业务一般无法正常响应算法验证，所以会存在很大的误拦截的风险。
- 如果用户存在 API 业务或原生 App 类业务的 CC 防护需求，请 [提交工单](#) 进行防护策略定制。

操作步骤

默认情况下，用户的 DDoS 高防 IP 实例所防护的网站域名采用正常等级的 CC 防护策略，用户可以根据实际情况自由调整防护模式。

1. 登录 [DDoS 防护控制台](#)，在左侧导航栏中，选择 **DDoS 高防 IP > 防护配置**，在防护策略页面，单击 **CC 防护**。
2. 在 CC 防护页面中，定位到页面下方 HTTP CC 防护和 HTTPS CC 防护区域，选择对应协议下需要开启 CC 防护的域名，设置 CC 防护等级。

HTTP CC防护

防护状态  对于敏感业务，可将业务URL添加到URL白名单，对该业务不做CC攻击检测和防护

http请求数阈值 当http请求数超过设定值时，触发CC防护。

选择防护域名

防护等级 ⓘ 宽松 正常 严格

HTTPS CC防护

选择防护域名

防护状态  对于敏感业务，可将业务URL添加到URL白名单，对该业务不做CC攻击检测和防护

https请求数阈值 当指定域名收到的https请求数超过设定值时，触发CC防护

防护等级 ⓘ 宽松 正常 严格

① 注意：

- CC 防护等级策略仅对接入配置为网站业务（七层接入）的域名生效。
- 如果用户还未将需要配置的网站域名接入高防 IP 实例，请参考 [接入网站业务](#) 将域名添加至已购买的高防 IP 实例。

更多信息请参考 [管理 CC 防护策略](#)。

管理 CC 防护策略

最近更新时间：2025-08-07 17:59:42

DDoS 高防 IP 支持 HTTP/HTTPS CC 防护功能。当高防 IP 统计的 HTTP/HTTPS 请求量超过设定的 **http/https 请求数阈值** 时，将自动触发 HTTP/HTTPS CC 防护。

DDoS 高防 IP 提供设置访问控制策略功能。开启 HTTP/HTTPS CC 防护功能，用户可以使用常见 HTTP/HTTPS 报文的字段（如 host 参数、CGI 参数、Referer 和 User-Agent 等）设置匹配条件，对公网用户的访问请求进行管控，对命中条件的请求执行阻断、人机识别动作。用户也可以设置限速规则，对访问 IP 执行限速处理。

DDoS 高防 IP 还支持 URL 白名单、IP 白名单、IP 黑名单策略配置：

- 白名单中的 URL，其访问请求将无需执行 CC 攻击检测，直接被放行。
- 白名单中 IP，其 HTTP/HTTPS 访问请求将无需执行 CC 攻击检测，直接被放行。
- 黑名单中 IP，其 HTTP/HTTPS 访问请求将直接被拒绝。

开启CC防护

HTTP CC 防护

1. 登录 [DDoS 防护管理控制台](#)，在左侧导航中选择 **DDoS 高防 IP > 防护配置**，在防护配置页面下，单击 **CC 防护**，选择目标实例。
2. 在 **HTTP CC 防护** 区域，单击 **防护状态** 右侧的  开启 HTTP CC 防护，单击 **http 请求数阈值** 右侧的下拉框选择合适的阈值即可。

HTTP CC防护

防护状态



对于敏感业务，可将业务URL添加到URL白名单，对该业务不做CC攻击检测和防护

http请求数阈值

100 QPS

▼

当http请求数超过设定值时，触发CC防护。

① 说明：

CC 防护状态默认关闭。防护状态开启后，才可设置 HTTP 请求数阈值。

HTTPS CC 防护

1. 登录 [DDoS 防护管理控制台](#)，在左侧导航中选择 **DDoS 高防 IP > 防护配置**，在防护配置页面下，单击 **CC 防护**，选择目标实例。

- 在 **HTTPS CC** 区域，选择防护域名，单击**防护状态**右侧的  开启 HTTPS CC 防护，单击 **https 请求数阈值** 右侧的下拉框选择合适的阈值。

HTTPS CC防护

选择防护域名

test. 

防护状态

 对于敏感业务，可将业务URL添加到URL白名单，对该业务不做CC攻击检测和防护

https请求数阈值

850 QPS 

当指定域名收到的https请求数超过设定值时，触发CC防护

说明：

CC 防护状态默认关闭。防护状态开启后，才可设置 HTTPS 请求数阈值。

自定义 CC 防护策略

说明：

- 需要开启 HTTP/HTTPS CC 防护，才可设置自定义 CC 防护策略，最多可添加5条。
- 仅在该高防 IP 正在遭受CC攻击时，自定义策略才会生效。
- 匹配模式下，每个自定义策略最多可以设置4个策略条件进行特征控制，且多个条件之间是“与”的关系，需要所有条件全部匹配策略才生效。
- 限速模式下，每个自定义策略只允许设置1条策略条件。

- 登录 [DDoS 防护管理控制台](#)，在左侧导航中，选择**DDoS 高防 IP>防护配置**，进入防护配置页面，单击**CC 防护**，选择地域和线路，选择目的实例，单击**添加访问控制策略**。

2. 在添加访问控制策略弹出框，根据实际业务需求设置以下参数，单击确定即可。

添加访问控制策略

请添加需要访问控制策略，添加完成后默认开启该策略

策略名称

请输入策略名称，最长20个字

协议

☒ HTTP
 ☐ HTTPS

模式

☒ 匹配模式
 ☐ 限速模式

策略

当

host

包含

时

+添加一行

执行

拦截

确定

取消

- 策略名称
输入策略名称，长度为1 – 20字符，不限制字符类型。
- 协议
目前支持 HTTP、HTTPS 两种协议。
- 防护域名
只有勾选 HTTPS 协议，才需要选择对应的防护域名。可选择的防护域名范围，等于已完成配置的转发规则中，属于 HTTPS 协议的网站域名。
- 模式
 - 匹配模式：匹配到 HTTP / HTTPS 对应字段头的请求，执行拦截或人机识别操作。
 - 限速模式：对源 IP 访问进行限速处理，HTTPS 协议不支持选择限速模式。
- 策略
 - 当选择匹配模式时，协议是 HTTP，支持从 HTTP 报文的 host 参数、CGI 参数、Referer 和 User-Agent 多个特征进行组合，组合逻辑包括包含、不包含和等于。最多可以设置4个策略条件进行特征控制。若协议是 HTTPS 时，支持从 HTTPS 报文的 CGI 参数、Referer 和 User-Agent 多个特征进行组合，组合逻辑包括包含、不包含和等于。最多可以设置3个策略条件进行特征控制，字段描述如下：

匹配字段	字段描述	适用的逻辑符
host	访问请求的域名。	包含、不包含、等于

CGI	访问请求的 URI 地址。	包含、不包含、等于
Referer	访问请求的来源网址，表示该访问请求是从哪个页面跳转产生的。	包含、不包含、等于
User-Agent	发起访问请求的客户端浏览器标识等相关信息。	包含、不包含、等于

- 当选择**限速模式**时，对每个源 IP 访问进行限速处理。只允许设置1个策略条件。

模式

☐ 匹配模式
 ☒ 限速模式

请慎用限速模式，该模式自定义策略只能添加一条

策略

每个源IP的访问速率

 次/分钟

- 执行

仅当选择**匹配模式**时，需要设置该参数。表示策略匹配后，需执行的处理动作，包括拦截和验证码。

设置黑白名单

1. 登录 [DDoS 防护管理控制台](#)，在左侧导航中，选择 **DDoS 高防 IP > 防护配置**，进入防护配置也页面，单击 **CC 防护**，选择地域和线路，选择目的实例。
2. 勾选页面右侧 **HTTP** 或 **HTTPS**，选择 **URL 白名单**、**IP 白名单**或 **IP 黑名单**，进行黑白名单设置，支持添加、修改，也支持批量导入导出。

URL白名单

IP白名单

IP黑名单

添加 URL

批量导入

批量导出

删除

最多可以添加50条URL

HTTP

HTTPS

☐	URL	协议	域名	操作
☐		http	-	删除
☐		http	-	删除

配置健康检查

最近更新时间：2023-07-21 09:44:42

操作场景

DDoS 高防 IP 通过健康检查帮助用户自动识别后端服务器的运行状况，自动隔离异常的服务器。以此降低了后端服务器异常对整体业务可用性的影响。

● 非网站业务（四层）健康检查

DDoS 高防 IP 非网站业务防护的健康检查机制，由高防集群节点向配置中指定的服务器端口发起访问请求，如果端口访问正常则视为后端服务器运行正常，否则视为后端服务器运行异常。

在 TCP 协议下，探测端口能否连接；在 UDP 协议下，使用 ping 进行可达性检查。

● 网站业务（七层）健康检查

DDoS 高防 IP 网站业务防护的健康检查机制，由高防转发集群向后端服务器发送 HTTP 请求的方式来检查后端服务，高防系统根据 HTTP 返回状态码来判断服务是否正常。

用户可以自定义设置响应代码所代表的状态。假定在某场景下，HTTP 返回值为 http_1xx、http_2xx、http_3xx、http_4xx 和 http_5xx，用户可以根据业务需要勾选 http_1xx 及 http_2xx 为服务正常状态，则返回 http_3xx 至 http_5xx 的值则代表异常状态。

① 说明：

配置四层或七层转发规则时，如果单条规则中仅配置1个源站 IP，健康检查功能将不开启，该功能适合多源站 IP 的情况下开启。

操作步骤

非网站业务健康检查配置

下面将为您介绍配置 DDoS 高防 IP 非网站业务防护的健康检查规则的详细步骤。

1. 登录 [DDoS 防护控制台](#)，在左侧导航栏中，选择 **DDoS 高防 IP > 接入配置**，进入管理页面。
2. 单击**非网站业务**，选择目的 DDoS 高防 IP 实例和相应规则，单击健康检查列下的**编辑**。



3. 在健康检查编辑页面，单击**显示高级选项**，设置配置项后，单击**确定**即可。



健康检查编辑

健康检查 ☒

隐藏高级选项 ▼

响应超时 秒 (0秒 - 60秒)

检测间隔 秒 (0秒 - 300秒)

不健康阈值 次 (0次 - 10次)

健康阈值 次 (0次 - 10次)

确定 **取消**

① 说明：

- 默认开启健康检查。
- 在配置健康检查时，建议使用默认值。
- 支持对健康检查配置信息批量导入导出。导入后，系统将根据导入的“转发协议、转发端口”与规则进行一一匹配，其中“转发端口”必须为已配置了规则的转发端口。

网站业务健康检查配置

下面将为您介绍配置 DDoS 高防 IP 网站业务防护的健康检查规则的详细步骤。

1. 登录 [DDoS 防护控制台](#)，在左侧导航栏中，选择 **DDoS 高防 IP > 接入配置**，进入管理页面。

2. 单击**网站业务**，选择目的 DDoS 高防 IP 实例和相应规则，单击健康检查列下的**编辑**。

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
bgp1p-000001zj/1:

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	健康检查	状态
☐		http	80	1	关闭 编辑	成功

3. 在健康检查编辑页面，单击  开启健康检查功能，同时单击**显示高级选项**，进行配置项设置，确认无误后，单击**确定**即可。

健康检查编辑

健康检查 

隐藏高级选项

检测间隔
10秒
60秒
15 秒

不健康阈值
0次
10次
3 次

健康阈值
0次
10次
3 次

URL
/

HTTP请求方式
HEAD

HTTP状态码检测
☒ http_1xx
☒ http_2xx
☒ http_3xx
☒ http_4xx
☐ http_5xx

当状态码为http_1xx、http_2xx、http_3xx、http_4xx，认为后端服务器存活

确定
取消

说明：

- 默认关闭健康检查。
- 在配置健康检查时，建议使用默认值。

- 支持批量导入导出健康检查配置信息。导入后，系统将根据导入的“转发协议、业务域名”与规则进行一一匹配，其中“业务域名”必须为已配置了规则的业务域名。

配置项说明

四层健康检查

配置项	说明
响应超时	每次健康检查响应的最大超时时间。如果后端服务器在指定的时间内没有正确响应，则判定为健康检查失败。
检测间隔	进行健康检查的时间间隔。
不健康阈值	在健康检查状态为成功时，连续 n 次（n 为填写的数值）收到健康检查失败状态，则识别为不健康，控制台显示异常。
健康阈值	在健康检查状态为失败时，连续 n 次（n 为填写的数值）收到健康检查成功状态，则识别为健康，控制台无显示。

七层健康检查

配置项	说明
检测间隔	进行健康检查的时间间隔，默认为15秒。
不健康阈值	在健康检查状态为成功时，连续 n 次（n 为填写的数值）收到健康检查失败状态，则识别为不健康，控制台显示异常。
健康阈值	在健康检查状态为失败时，连续 n 次（n 为填写的数值）收到健康检查成功状态，则识别为健康，控制台无显示。
HTTP 请求方式和检查路径 URL	默认使用 HEAD 方法，服务器仅返回响应消息报文头。使用 GET 方法，服务器返回完整的响应消息。对应后端服务器需要支持 HEAD 和 GET。 - 如果用来进行健康检查的页面并不是应用服务器的缺省首页，用户需要指定具体的检查路径。 - 如果对 HTTP HEAD 请求限定了 host 字段的参数，用户需要指定检查路径，即用于健康检查页面文件的 URI。
HTTP 状态码检测	判断健康检查是否正常的 HTTP 状态码。默认情况或不做任何选择时，该值为 http_1xx、http_2xx、http_3xx 和 http_4xx，如果 HTTP 返回状态码非默认状态值，则识别为不健康，支持修改。

配置会话保持

最近更新时间：2023-07-21 09:44:42

操作场景

DDoS 高防 IP 非网站业务防护提供基于 IP 地址的会话保持，支持将来自同一 IP 地址的请求转发到同一台后端服务器处理。

四层转发场景支持简单会话保持能力，会话保持时间可设为30 – 3600秒中的任意整数值。超过该时间阈值，会话中无新的请求则自动断开连接。

操作步骤

下面将为您介绍配置 DDoS 高防 IP 非网站业务防护的健康检查规则的详细步骤。

1. 登录 [DDoS 防护控制台](#)，在左侧目录中，单击 **DDoS 高防 IP> 接入配置**，进入管理页面。
2. 在**非网站业务**页签，选择目的 DDoS 高防 IP 实例和相应规则，单击其会话保持查列下的**编辑**。

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

华东地区(上海)

BGP

bgpip-00000210/

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	水印剥离状态
☐	TCP/4430	443		加权轮询	开启 编辑	关闭 编辑	关闭

3. 在**会话保持编辑**页面，单击按钮 开启会话保持功能，设置保持时间后，单击**确定**即可。

会话保持编辑

×

会话保持 ⓘ

☒

保持时间 ⓘ

0秒

3600秒

0

秒

确定

取消

① 说明：

- 默认关闭会话保持。
- 在设置保持时间时，建议使用默认值。
- 支持对会话保持配置信息批量导入导出。导入后，系统将根据导入的“转发协议、转发端口”与规则进行一一匹配，其中“转发端口”必须为已配置了规则的转发端口。

配置智能调度

最近更新时间：2024-11-08 09:20:52

应用场景

一般每个账号下可能拥有多个高防实例，且每个高防实例至少拥有一条高防线路，因此每个账号下可能会存在多条高防线路。当将业务添加至高防实例进行防护后，表示您已经为该业务配置一条高防线路作为防护线路。若您的业务配置存在多条高防线路作为防护线路，您需要考虑该业务流量的调度方式，即如何将业务流量调度到最优的高防线路进行防护，保证业务访问速度和高可用性。

目前 DDoS 防护服务提供优先级方式的 CNAME 智能调度功能，您可以根据实际需要，勾选高防实例并设置高防线路的优先级。

① 说明：

支持设置解析的高防实例有 DDoS 高防包、DDoS 高防 IP 和 DDoS 高防 IP 专业版，其中 DDoS 高防包包括独享包和共享包。

优先级调度方式

指针对所有的 DNS 请求均以优先级最高的高防线路进行响应，即所有访问流量被调度至当前优先级最高的高防线路。您可以编辑高防线路的优先级，默认优先级为100，优先级的值越小，则表示该高防线路优先级越高。具体调度规则如下：

- 如果业务配置的高防实例包含多条不同高防线路，且优先级相同时，则按照 DNS 请求的运营商来源进行响应。当其中某条高防线路遭遇封堵后，将按照 BGP > 电信 > 联通 > 移动 > 境外（包括中国香港、中国台湾）的线路顺序进行调度。
- 如果同一优先级的高防线路均遭遇封堵后，访问流量将自动调度到当前可用的优先级次高的高防线路。

① 注意：

若当前无次高优先级的高防线路可用，则无法进行自动调度，业务访问将会中断。

- 如果业务配置的高防实例，包含多条相同高防线路，且优先级相同时，则按负载均衡方式进行调度，将访问流量平均分发至这些相同运营商的高防线路上进行处理。

示例

假设您拥有高防实例：BGP 高防 IP 1.1.1.1和1.1.1.2、电信高防 IP 2.2.2.2、联通高防 IP 3.3.3.3，其中 1.1.1.1、2.2.2.2和3.3.3.3的优先级都为1，1.1.1.2的优先级为2。正常情况下，所有流量被调度至当前优先级为1的一组高防线路进行分发处理，因此来自联通的流量调度到3.3.3.3进行处理，来自电信的流量调度到 2.2.2.2进行处理，来自其他运营商的流量调度到1.1.1.1进行处理。当1.1.1.1进入封堵时，该 IP 下的访问流量将自动调度到 2.2.2.2进行处理，当1.1.1.1和3.3.3.3都被封堵时，则原本调度至1.1.1.1和3.3.3.3的访问流量，都将分发至 2.2.2.2进行处理，当该组高防线路全部进入封堵时，流量将被调度至1.1.1.2进行处理。

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。

说明：

- 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 高防包 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 高防 IP 接入非网站业务](#) 或 [接入网站业务](#)。

- 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 [云解析 DNS](#)。

设置线路优先级

请参考以下步骤，按照设想的调度方案为您的高防线路设置优先级：

- 登录 [DDoS 防护管理控制台](#)，在左侧导航栏选择智能调度>域名列表，进入域名列表页面，单击创建智能调度，系统自动生成一个 CNAME 记录。



- 找到该 CNAME 记录所在行，单击添加高防实例，进入智能调度编辑页面。



3. 在智能调度编辑页面中，TTL 值默认60秒，取值范围为1 – 3600（秒），调度方式为默认优先级。

智能调度编辑

CNAME

TTL值

60秒 [调整](#)

调度方式

优先级

IP资源和解析设置

[添加高防实例](#)

4. 进入添加高防实例页面，勾选需要设置高防线路优先级的实例，可选高防实例包括独享包、共享包、DDoS 高防 IP 和 DDoS 高防 IP 专业版，单击确定。

添加高防实例

选择IP

高防IP专业版

独享包

共享包

高防IP

高防IP专业版

输入ID/

☐

资源类型

☒

net-00000025

高防IP专业版

☒

net-00000024

高防IP专业版

☐

net-00000024

高防IP专业版

☐

net-00000024

高防IP专业版

☐

net-00000024

高防IP专业版

☐

net-00000023

高防IP专业版

已选择(4)

资源ID/名称	IP地址	资源类型	
bgp-00000046		独享包	×
bgpip-00000101		高防IP	×
net-00000025		高防IP专业版	×
net-00000024		高防IP专业版	×

确定

取消

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。

智能调度编辑

CNAME4ion6w7a

TTL值60秒 调整

调度方式优先级

IP资源和解析设置添加高防实例

资源ID	IP地址	线路	优先级	地区	运行状态	域名解析	操作
net-00000		BGP	100	华东地区(上海)	运行中	☒	解除绑定
net-00000		BGP	100	华东地区(上海)	运行中	☒	解除绑定
bgpip-00000		电信	100	华东地区(上海)	运行中	☒	解除绑定
bgp-00000		BGP	100	华东地区(上海)	运行中	☒	解除绑定

100

确定 取消

示例

例如，您想要将业务流量先调度到 BGP 高防线路，当 BGP 高防线路被攻击遭到封堵后，将流量自动调度到电信高防线路。如果电信高防线路也被封堵，则将流量调度到联通高防线路。当 BGP 高防线路的封堵解除后，流量将自动恢复调度至 BGP 高防线路。

优先级设置方式：您可以将防护业务的高防实例中属于 BGP 高防线路的优先级设置成1、电信高防线路的优先级设置成2、联通高防 IP 线路的优先级不变，即可满足上述调度方案。

资源ID	IP地址	线路	优先级	地区	运行状态	域名解析	操作
net-00000		联通	100	华东地区(上海)	运行中	☒	解除绑定
bgpip-00000		电信	2	华东地区(上海)	运行中	☒	解除绑定
bgp-00000		BGP	1	华东地区(上海)	运行中	☒	解除绑定

如果您暂时不希望联通高防 IP 线路加入流量调度机制，单击 ☐ 关闭域名解析即可，后面再根据需要重新开启域名解析并设置优先级。若想从当前调度机制中剔除该线路，可直接找到该线路对应实例所在行，单击解除绑定即可。

修改 DNS 解析

使用 CNAME 智能调度前，建议您将业务域名 DNS 的 CNAME 记录，修改为 DDoS 防护智能调度系统自动生成的 CNAME，使所有用户访问业务网站的流量都牵引至高防系统。

1. 登录腾讯云 [DNS 解析 DNSPod 控制台](#)，在左侧导航栏中，单击**域名解析列表**，在域名解析列表页面，找到目标域名所在行，单击**解析**。

☐	域名	解析状态 ^①	解析套餐	最后操作时间	操作
☐		域名 DNS 未修改 ^①	个人专业版 2019-09-17 到期	2018-09-17 19:42:28	解析 升级套餐 更多 ▼
☐		域名 DNS 未修改 ^①	企业旗舰版 2020-01-22 到期	2018-01-22 11:13:50	解析 升级套餐 更多 ▼

2. 选择**记录管理**>**添加记录**，记录类型选择 CNAME，记录值内输入智能调度系统自动生成的 CNAME 地址，单击**保存**。

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

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 [↗](#)
请到域名注册商处将DNS修改为：ns3.dnsv5.com 和 ns4.dnsv5.com 后
修改DNS服务器需要最长72个小时的全球生效时间，请耐心等待。
遇到问题？查看FAQ文档 [↗](#)

添加记录 快速添加网站/邮箱解析 暂停 开启 删除 分配至项目

请输入您要搜索的记录

☐	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
☐	*	CNAME	默认	点击查看地址	-	600	-	保存 取消

配置攻击告警阈值

最近更新时间：2023-07-21 09:44:42

应用场景

当您所使用的 DDoS 高防 IP 遭受攻击、受攻击结束、被封堵以及解除封堵时，系统将以站内信、短信、邮件或微信的方式向您推送攻击告警信息。为更加合理、准确地推送攻击告警信息，减少困扰，新增攻击告警阈值配置功能。

若检测的指标超过您设定的阈值，将触发告警，并向您推送攻击告警信息。若发生正常业务操作（如同步数据等）引起流量突增，但被判定为攻击的情况，该功能可以较好地过滤这类情况，帮助您更加准确、清晰地掌握当前业务遭受的攻击状况。如何接收告警信息，请参见 [设置安全事件通知](#)。

配置 DDoS 攻击告警阈值

本配置示例可实现如下功能：DDoS 高防 IP 实例“bgpip-0000021y”遭受的攻击流量超过清洗阈值触发 DDoS 攻击清洗，当累计的清洗流量（值）超过1000Mbps时，将向指定用户群体发送 DDoS 攻击告警信息。

注意：
需要开启 DDoS 防护状态，才可设置攻击告警阈值。

1. 登录 [DDoS 防护控制台](#)，在左侧导航栏中，选择 **DDoS 高防 IP > 资产列表**，进入高防 IP 页面，找到高防 IP 实例“bgpip-0000021y”，单击实例所在行的操作项**防护配置**。



2. 进入 DDoS 防护配置页面，在 DDoS 攻击告警阈值右侧的下拉框，选择告警指标**清洗流量**，并设置阈值为1000Mbps。

注意：
DDoS 攻击告警阈值默认未设置，支持可选的告警指标有**入流量带宽**和**清洗流量**。

DDoS防护配置

防护状态

☒

清洗阈值 ⓘ

60Mbps

▼

防护等级 ⓘ

宽松

正常

严格

业务场景

无

▼

高级策略

无

▼

DDoS攻击告警阈值

清洗流量

▼

1000

Mbps

配置 CC 攻击告警阈值

本配置示例可实现如下功能：DDoS 高防 IP 实例“bgpip-0000021y”触发 CC 防护后，当 HTTP CC 防护峰值超过2000QPS时，将向指定用户群体发送 CC 攻击告警信息。

① 注意：

需要开启 HTTP CC 防护状态，才可设置攻击告警阈值。

1. 登录 [DDoS 防护控制台](#)，在左侧导航栏中，选择DDoS 高防 IP>防护配置，进入防护配置页面，单击CC 防护。
2. 在 CC 防护页面中，定位到页面下方的“HTTP CC 防护”区域，在“HTTP CC 攻击告警阈值”处设置阈值为2000QPS。

HTTP CC防护

防护状态

☒

对于敏感业务，可将业务URL添加到URL白名单，对该业务不做CC攻击检测和防护

http请求数阈值

1500 QPS

▼

当http请求数超过设定值时，触发CC防护。

HTTP CC攻击告警阈值

2000

QPS

查看统计报表

最近更新时间：2025-08-07 17:59:42

当用户收到 DDoS 攻击提醒信息或发现业务出现异常时，需要快速了解攻击情况，包括流量大小、当前防护效果等，在掌握足够信息后，才可以采取更有效的处理方式，第一时间保障业务正常。

DDoS 高防 IP 管理控制台的统计报表提供丰富的信息，可帮助用户快速了解当前业务或攻击情况。

查看 DDoS 攻击防护情况

1. 登录 [DDoS 防护管理控制台](#)。
2. 定位到 **DDoS 高防 IP > 统计报表**。
3. 在 **DDoS 攻击防护**页签，设置查询时间范围，选择地域和线路，选择目的实例和高防 IP，查看是否存在攻击。

说明：

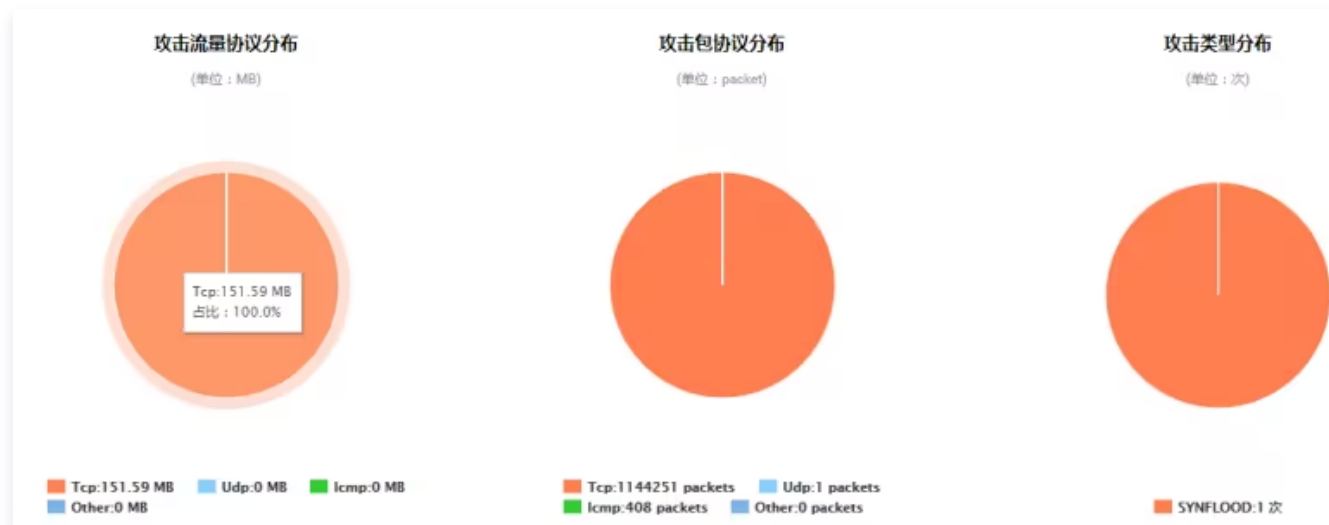
支持查询最多180天以内的攻击流量信息及 DDoS 攻击事件。

- 查看该时间范围内所选择的高防 IP 遭受的攻击情况，包括网络**攻击流量带宽 / 攻击包速率**趋势。当遭受攻击时，在流量趋势图中可以明显看出攻击流量的峰值。

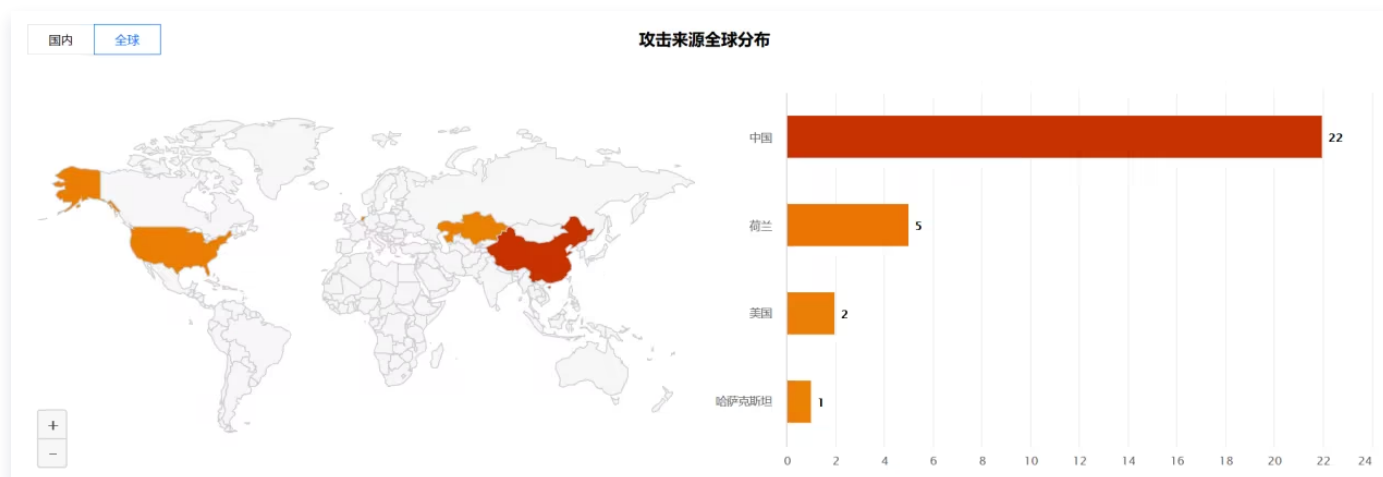


- 通过攻击流量协议分布、攻击包协议分布和攻击类型分布，查看这三个数据维度下的攻击分布情况。
 - 攻击流量协议分布：查看该时间范围内，所选择的高防 IP 遭受攻击事件中各协议总攻击流量的占比情况。
 - 攻击包协议分布：查看该时间范围内，所选择的高防 IP 遭受攻击事件中各协议攻击包总数的占比情况。

- **攻击类型分布：**查看该时间范围内，所选择的高防 IP 遭受的各攻击类型总次数占比情况。



- **攻击来源分布：**在攻击来源分布区域查看该时间范围内所遭受的 DDoS 攻击事件的攻击源在国内、全球的分布情况，便于用户清晰了解攻击来源情况，为进一步防护措施提供基础依据。



- 在 **DDoS 攻击记录** 区域查看该时间范围内所遭受的 DDoS 攻击事件，了解每一次攻击事件的攻击（开始）时间、持续时间、攻击类型以及攻击状态。
 - 支持攻击包下载，供用户进行 DDoS 攻击分析及溯源支撑。
 - 单击攻击详情，了解 DDoS 攻击事件中的最大包速率、最大攻击流量带宽和总的清洗流量情况。
 - 单击攻击源信息，查看该时间范围内，所遭受攻击的攻击源 IP 地址、来源地区、产生的攻击流量及攻击包量大小等信息。

① **注意：**

攻击源信息为抽样数据，即随机抓包统计的数据，在攻击结束后大约2小时才会显示数据。

DDoS攻击记录

攻击时间	持续时间	攻击类型	攻击状态	操作
▶ 2019-08-03 17:08:00	2分钟	SYNFLOOD	攻击结束	攻击包下载 攻击详情 攻击源信息
▶ 2019-08-02 09:58:00	2分钟	SYNFLOOD	攻击结束	攻击包下载 攻击详情 攻击源信息

查看 CC 攻击防护情况

1. 登录 [DDoS 防护管理控制台](#)。
2. 选择 **DDoS 高防 IP > 统计报表**。
3. 单击 **CC 攻击防护** 页签，设置查询时间范围，选择地域和线路，选择目的实例和高防 IP，查看是否存在 CC 攻击。

① 说明：

支持查询最多180天以内的攻击请求数信息及 CC 攻击事件。

- 用户可以选择今天查看所选择的高防IP的攻击请求数趋势。通过观察总请求值是否远高于正常情况下的业务访问量（QPS），并查看攻击 QPS 是否有数值且数值超大。
- 如果存在 CC 攻击，系统会记录下攻击的开始时间、结束时间、被攻击域名、被攻击 URL、总请求峰值、攻击请求峰值和攻击源等信息。
 - **总请求峰值**：统计遭受攻击时，高防 IP 接收到的总请求流量峰值。

- **攻击请求峰值**：统计遭受攻击时，由高防系统阻断的请求次数峰值。



查看业务流量情况

1. 登录 [DDoS 防护管理控制台](#)。
2. 选择 **DDoS 高防 IP > 统计报表**。
3. 单击**业务**页签，设置查询时间范围，选择地域和线路，选择目的实例和高防 IP，查看所选择时间范围内的**入/出业务流量带宽趋势**、**入/出业务包速率的趋势**及**新建连接数或并发连接数的趋势**。同时，还可以查看该时间范围内的入/出方向的业务流量带宽峰值，及入/出方向的业务包速率峰值。
 - **并发连接数**：系统在某个时间点存在的已建立的全连接数。

- **新建连接数**：系统在1秒内建立的 TCP 连接数。



说明：
支持查询最多180天以内的业务信息。

查看操作日志

最近更新时间：2023-07-21 09:44:42

操作场景

DDoS 高防 IP 支持查看近90天内重要操作的日志，如有需要，您可以登录 [DDoS 防护管理控制台](#) 查看。可查看的日志包含以下类别：

- 转发规则变更操作日志
- DDoS 高级防护策略变更操作日志
- 清洗阈值调整日志
- 防护等级变更日志
- CC 防护策略变更操作日志
- 弹性防护峰值调整日志
- 资源名称的修改日志

操作步骤

1. 登录 [DDoS 防护管理控制台](#)。
2. 选择**操作日志**，进入操作日志查询页面。
3. 设置时间范围，通过**产品类型**筛选**高防 IP**，查看对应的操作记录。

操作日志						
今天 昨天 近7天 近15天 近30天 2018-11-08 至 2018-12-07 回 请输入资源ID/账号 Q						
操作时间	对象ID	产品类型 ▼	操作内容	操作结果	操作账号	操作
2018-12-06 17:00:24		高防IP	批量删除4层转发规则	成功		展开
2018-12-06 15:49:20		高防IP	删除4层转发规则	成功		展开
2018-12-06 15:36:44		高防IP	添加4层转发规则	成功		展开
2018-12-06 15:36:19		高防IP	添加4层转发规则	成功		展开
2018-12-06 15:06:58		高防IP	修改DDoSIP防护等级	成功		展开

设置安全事件通知

最近更新时间：2023-07-21 09:44:42

操作场景

当您使用的高防 IP 受到攻击、受攻击结束、IP 被封堵以及解除封堵时，将以站内信、短信、邮件、微信或者电话的方式，向您推送告警信息：

- 攻击开始时，您将会收到攻击开始提示。
- 攻击结束后15分钟，您将收到攻击结束提示。
- IP 被封堵时，您将收到封堵提示。
- IP 解除封堵时，您将收到解除封堵提示。

您可以根据实际情况修改告警信息的接收人和接收方式。

操作步骤

1. 登录您的腾讯云账号，进入 [消息中心](#)。

① 说明：

您也可以登录 [控制台](#)，单击右上角的 ，在弹出页面单击[查看更多](#)，进入消息中心。

2. 在左侧目录中单击[消息订阅](#)，进入消息列表。
3. 在消息列表中，在安全事件通知所在列，选择接收方式，单击[修改消息接收人](#)，进入修改消息接收人页面。

添加接收人		移除接收人									
消息类型				☐ 站内信	☐ 邮件	☒ 短信	☐ 微信	☐ 企业微信	☐ 语音	接收人	操作
▸ ☐ 财务消息											
▸ ☐ 产品消息											
▼ ☐ 安全消息											
☐ 安全事件通知		☒	☒	☒	☒	☐	☐			腾讯云安全技术支持	修改消息接收人
产品遭受（如DDoS）攻击、服务器对外（如DDoS）攻击/扫描导致被隔离等安全事件的通知		☒	☒	☐	☐	☐	☐			腾讯云安全技术支持	修改消息接收人

4. 在修改消息接收人页面，进行消息接收人的设置，设置完成后单击确定即可。

修改消息接收人

① 邮箱、手机、微信未验证的用户将无法接收邮件、短信、语音、微信消息，验证通过并开启对应接收方式后即可接收
非企业微信子用户无法接收企业微信消息，企业微信子用户且在腾讯云助手应用的成员可见范围内方可接收企业微信消息。

消息类型

安全事件通知

接收人

用户

用户组

新增消息接收人

修改接收人联系方式

搜索用户名称

Q

☒	用户名称	用户类型	手机号码	邮箱	微信
☒	1				

已选择(1)

确定

取消

实践教程

平滑切换线上业务至 DDoS 高防 IP

最近更新时间：2023-07-21 09:44:43

需求背景

已上线的业务可能存在较多的特定设置和限制条件，且业务中断影响较大。因此建议用户将已上线运行的业务切换到本产品之前，参考本节相关建议，采用合适的切换方式，规避可能存在的风险。

建议

① 注意：

以下建议是基于腾讯云过往线上业务切换而总结的相关经验，用户需结合自身实际业务情况进行完善和补充，确保将切换过程中的风险降至最低。

技术维度

- 通过本地修改 hosts 文件来替代直接修改 DNS A 记录，由测试人员本地进行业务测试，验证可用性，测试延时等相关指标。
- 若已使用智能域名解析产品，可基于部分运营商或部分地域进行 DNS A 记录修改，先小范围将流量牵引到高防 IP 灰度上线再逐步完成全部业务切换。
- 减小 DNS 的 TTL，一旦出现问题可尽快切回。
- 提前准备回退方案，一旦出现问题可根据回退方案有序操作。

业务维度

- 选取备份业务、非重要业务、非关键业务先进行迁移。
- 选择业务较少的时段进行迁移。

源站 IP 暴露的解决方法

最近更新时间：2023-07-21 09:44:43

由于部分攻击者会记录源站使用过的 IP，因此在使用 DDoS 高防 IP 后，如果还存在绕过高防直接攻击源站 IP 的情况，建议更换源站 IP。

如不想更换源站 IP 或已经更换过 IP 但仍存在 IP 暴露情况，为防止出现攻击绕过高防直接攻击源站 IP 的情况，强烈参考下面方法以保护源站 IP：

- 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。
- 提前准备备份链路和备份 IP。
- 设置访问来源范围，避免攻击者的恶意扫描。
- 参考 [与源站结合的防护调度方案](#)，结合实际情况进行应用。

① 说明：

更换源站 IP 之前，请务必确认已消除所有可能暴露源站 IP 的因素。

在更换源站 IP 前可参考下列检查方法，对暴露源站 IP 的可能因素进行逐一排查，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、后门检查

检查源站服务器是否存在木马、后门等隐患。

获取客户端真实 IP（域名接入）

最近更新时间：2025-08-08 14:31:52

本文档将为您介绍通过 DDoS 高防直接获取真实 IP 的方法，以及针对 Tomcat、Apache、Nginx 和 IIS 服务器，介绍相应的 X-Forwarded-For 配置方案及获取真实 IP 的方法。

背景信息

通常情况下，当用户进行网站访问时，浏览器可能不是直达服务器，中间会部署 CDN 及 DDoS 高防等防护服务。例如，采用这样的架构：“用户 > CDN/DDoS 高防 > 源站服务器”。

如果您已经使用 DDoS 高防服务，可直接通过高防服务获取访问者的真实 IP，您也可以通过配置网站服务器来获取访问者的真实 IP。DDoS 高防 IP 使用网站业务转发规则时，可利用 HTTP 头部的 X-Forwarded-For 字段获取客户端真实 IP。

X-Forwarded-For：是一个 HTTP 头部扩展字段，目的是使服务器可以识别通过代理等方式连接的客户端真正的 IP。

格式为：X-Forwarded-For: Client, proxy1, proxy2, proxy3……

当高防 IP 将用户的访问请求转到后端服务器时，会把请求用户的真实 IP 记录在 X-Forwarded-For 字段的首位。因此，源站应用只需要获取 HTTP 头部的 X-Forwarded-For 字段的内容即可。

通过 HTTP Header 获取真实 IP

DDoS 高防服务默认提供获取客户端真实 IP 的功能，下面推荐两种方式获取客户的来源 IP，您可以根据需要，选择任意一种方式进行使用：

- **方式1：**DDoS 高防服务使用 X-Forwarded-For 的方式获取客户端的真实 IP 地址。
 - 真实的客户端 IP 会被 DDoS 高防服务放在 HTTP 头部的 X-Forwarded-For 字段，格式如下：

```
X-Forwarded-For: 用户真实IP, 代理服务器1-IP, 代理服务器2-IP, ...
```

① 说明：

当使用此方式获取客户端真实 IP 时，获取的第一个地址即为客户端真实 IP。

- 各语言通过调用 SDK 接口获取 X-Forwarded-For 字段的方式如下：
 - ASP:

```
Request.ServerVariables("HTTP_X_FORWARDED_FOR")
```

- ASP.NET(C#):

```
Request.ServerVariables["HTTP_X_FORWARDED_FOR"]
```

- PHP:

```
$_SERVER["HTTP_X_FORWARDED_FOR"]
```

- JSP:

```
request.getHeader("HTTP_X_FORWARDED_FOR")
```

- **方式2:** DDoS 高防服务支持使用 X-Real-IP 变量，获取客户的来源 IP（使用过程中考虑了后面所经过的多层反向代理对该变量的修改）。

各种语言通过调用 SDK 接口获取 X-Real-IP 字段的方式如下：

- ASP:

```
Request.ServerVariables("HTTP_X_REAL_IP")
```

- ASP.NET(C#):

```
Request.ServerVariables["HTTP_X_REAL_IP"]
```

- PHP:

```
$_SERVER["HTTP_X_REAL_IP"]
```

- JSP:

```
request.getHeader("HTTP_X_REAL_IP")
```

访问日志打印真实 IP

Tomcat 如何在访问日志中获取真实客户端的 IP 地址

如果您的源站部署了 Tomcat 服务器，可通过启用 Tomcat 的 X-Forwarded-For 功能，获取访问者的真实 IP 地址。

1. 打开 server.xml 文件（“tomcat/conf/server.xml”），AccessLogValve 日志记录功能部分内容如下：

```
<Host name="localhost" appBase="webapps" unpackWARs="true"
autoDeploy="true">
    <Valve className="org.apache.catalina.valves.AccessLogValve"
directory="logs"
    prefix="localhost_access_log." suffix=".txt"
    pattern="%h %l %u %t \"%r\" %s %b" />
```

2. 在 pattern 中增加 “%{X-Forwarded-For}i”，修改后的 server.xml 为：

```
<Host name="localhost" appBase="webapps" unpackWARs="true"
autoDeploy="true">
    <Valve className="org.apache.catalina.valves.AccessLogValve"
directory="logs"
    prefix="localhost_access_log." suffix=".txt"
    pattern="%{X-Forwarded-For}i %h %l %u %t \"%r\" %s %b" />
</Host>
```

3. 查看 localhost_access_log 日志文件，可获取 X-Forwarded-For 对应的访问者真实 IP。

Apache 如何在访问日志中获取真实客户端的 IP 地址

如果您的源站部署了 Apache 服务器，可通过运行命令安装 Apache 的第三方模块 mod_remoteip，并修改 httpd.conf 文件获取客户 IP 地址。

1. 打开 httpd.conf 配置文件，并将文件内容修改为如下内容：
Apache 映射 xff 到 remote_addr，详情请参见 [安装 mod_remoteip](#)。
2. 定义日志格式。

```
LogFormat "%{X-Forwarded-For}i %l %u %t \"%r\" %>s %b \"%{Referer}i\"
\"%{User-Agent}i\"" common
```

3. 重启 Apache，使配置生效。

```
/[apached目录]/httpd/bin/apachectl restart
```

4. 查看 access.log 日志文件，可获取 X-Forwarded-For 对应的访问者真实 IP。

Nginx 如何在访问日志中获取真实客户端的 IP 地址

如果您的源站部署了 Nginx 反向代理，可通过在 Nginx 反向代理配置 Location 信息，后端 Web 服务器即可通过类似函数获取客户的真实 IP 地址。

1. 根据源站 Nginx 反向代理的配置，在 Nginx 反向代理的相应 location 位置配置如下内容，获取客户 IP 的信息。

```
log_format main '$remote_addr [$http_x_forwarded_for]- $remote_user  
[$time_local] '   
                '$request' $status $body_bytes_sent '   
                '$http_referer' '$http_user_agent';
```

2. 重启 nginx。

通过插件映射客户端真实 IP

Tomcat 配置方案

Tomcat 配置 xff 映射到 remote_addr，详情请参见 [tomcat 配置文档](#)。

配置示例如下：

```
<Valve className="org.apache.catalina.valves.RemoteIpValve"  
remoteIpHeader="x-forwarded-for"  
proxiesHeader="x-forwarded-by"  
internalProxies="192\.168\.0\.10|192\.168\.0\.11"  
trustedProxies="62\.234\.227\. \d{1,3}|212\.64\.62\. \d{1,3}"  
>
```

Apache 配置方案

Apache 映射 xff 到 remote_addr，需 [安装 mod_remoteip](#) 进行操作。

配置示例如下：

```
RemoteIPHeader X-Forwarded-For  
RemoteIPTrustedProxyList x.x.x.x/24
```

IIS 6 配置方案

如果您的源站部署了 IIS 6 服务器，您可以通过安装 F5XForwardedFor.dll 插件，从 IIS 6 服务器记录的访问日志中获取访问者真实的 IP 地址。

1. 下载并安装 [F5XForwardedFor](#) 模块。

2. 根据您的服务器的操作系统版本将 x86\Release 或者 x64\Release 目录中的 F5XForwardedFor.dll 文件拷贝至指定目录（如 C:\ISAPIFilters），同时确保 IIS 进程对该目录有读取权限。
3. 打开 IIS 管理器，找到当前开启的网站，在该网站上右键单击**属性**，打开“属性”页面。
4. 在“属性”页面，切换至 ISAPI 筛选器，单击**添加**，在弹出的窗口中，配置如下信息：
 - **筛选器名称**：F5XForwardedFor。
 - **可执行文件**：F5XForwardedFor.dll 的完整路径，例如：C:\ISAPIFilters\F5XForwardedFor.dll。
5. 单击**确定**，重启 IIS 6 服务器。
6. 查看 IIS 6 服务器记录的访问日志（默认的日志路径为：C:\WINDOWS\system32\LogFiles\，IIS 日志的文件名称以 .log 为后缀），可获取 X-Forwarded-For 对应的访问者真实 IP。

IIS 7 配置方案

如果您的源站部署了 IIS 7 服务器，您可以通过安装 F5XForwardedFor 模块，从 IIS 7 服务器记录的访问日志中，获取访问者真实的 IP 地址。

1. 下载并安装 [F5XForwardedFor](#) 模块。
2. 根据服务器的操作系统版本将 x86\Release（或 x64\Release）目录中的 F5XFFHttpModule.dll 和 F5XFFHttpModule.ini 文件拷贝到指定目录（如 C:\x_forwarded_for\x86 或 C:\x_forwarded_for\x64），并确保 IIS 进程对该目录有读取权限。
3. 在 IIS 服务器的选择项中，双击**模块**，进入“模块”界面。
4. 单击**配置本机模块**，在弹出的对话框中，单击**注册**，按操作系统选择注册模块注册已下载的 DLL 文件。
 - x86 操作系统：注册模块 x_forwarded_for_x86
 - 名称：x_forwarded_for_x86
 - 路径：C:\x_forwarded_for\x86\F5XFFHttpModule.dll
 - x64 操作系统：注册模块 x_forwarded_for_x64
 - 名称：x_forwarded_for_x64
 - 路径：C:\x_forwarded_for\x64\F5XFFHttpModule.dll
5. 注册完成后，勾选新注册的模块（x_forwarded_for_x86 或 x_forwarded_for_x64）并单击**确定**。
6. 在 ISAPI 和 CGI 限制中，按操作系统添加已注册的 DLL 文件，并将其“限制”改为“允许”。
 - x86 操作系统：
 - ISAPI 或 CGI 路径：C:\x_forwarded_for\x86\F5XFFHttpModule.dll
 - 描述：x86
 - x64 操作系统：
 - ISAPI 或 CGI 路径：“C:\x_forwarded_for\x64\F5XFFHttpModule.dll”
 - 描述：x64
7. 重启 IIS 7 服务器，等待配置生效。

8. 查看 IIS 7 服务器记录的访问日志（默认的日志路径为：C:\WINDOWS\system32\LogFiles\，IIS 日志的文件名称以 .log 为后缀），可获取 X-Forwarded-For 对应的访问者真实 IP。

与源站结合的防护调度方案

最近更新时间：2023-07-21 09:44:43

需求背景

部分用户的业务对延时要求严格，或者受限于业务要求常态化情况下必须直接访问源站，此时可考虑结合源站的防护调度方案。

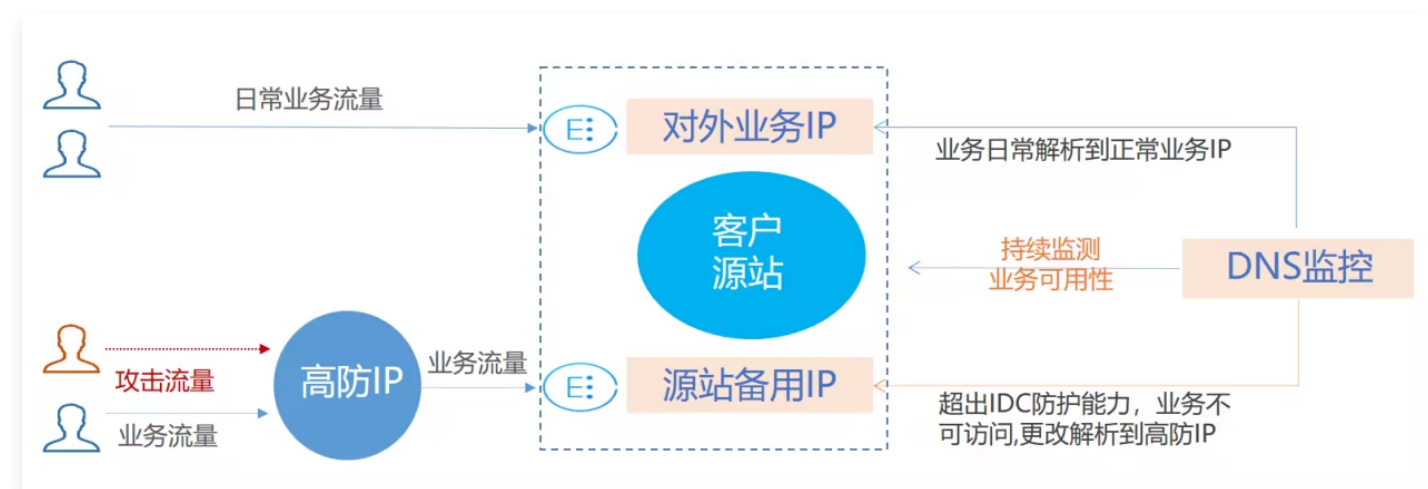
该方案可满足流量常态化情况下直接访问源站，但遭到攻击后可迅速具备防护能力的要求。

防护方案

与源站结合的防护调度方案如下图：

① 说明：

本方案依赖于 DNS 服务商，需要具备监控和智能切换功能。



方案说明

本方案主要由高防 IP、DNS 监控、客户源站的对外业务 IP 和源站备用 IP 组成。

- 常态化情况下，业务的域名解析到正常的对外业务 IP，业务流量直接访问源站。DNS 监控实时监控源站业务是否可以正常访问。
- 当 DNS 监控检测到正常的对外业务 IP 无法访问时，依据智能切换的设置规则，迅速将业务域名解析到高防 IP 上。高防 IP 对攻击流量进行清洗，将干净的业务流量转发到源站的备用 IP，从而保障业务可用。

① 注意：

为避免由于网络抖动等因素造成的误切换，确保监控效果，建议进行手动切换。

方案效果

- 满足常态化情况下直接访问源站的需求。
- 适用于对延时要求非常严格的业务。
- 遭到攻击超出源站防护能力后，可自动切换到高防 IP 进行防护。

建议与注意事项

- 需提前完成源站备用 IP、高防 IP 转发规则等配置。
- 建议将源站备用 IP 与正常的业务 IP 分布在不同的物理线路，以获得更好的防护效果。
- 建议定期进行验证和演练，熟悉方案细节，解决可能存在的问题。

业务系统压力测试建议

最近更新时间：2023-07-21 09:44:43

压力测试的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建议，再拟定合适实施方案。

① 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。

① 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。

SDK 文档

水印 SDK

最近更新时间：2025-08-08 14:31:52

本文将为您介绍如何接入水印 SDK，本文主要包括 Android、iOS 和 Windows 三个版本的接入指南。

SDK 准备

下载相关 [Demo](#) 及 [SDK](#)。

Android 接入

预备工作

- 接入 SDK 需要完成以下步骤：
 - 1.1 根据运行平台选择相应的 so 文件，将 so 文件和 jar 文件拷贝到工程目录下并添加依赖。
 - 1.2 调用 SDK 接口函数，生成水印信息。
 - 1.3 发送报文时，将20字节水印信息放在消息体前面。
- SDK 文件包含 so 文件和 jar 文件，目录结构如下：



- SDK API 说明：
 - 程序包：com.gamesec
 - 类：Mark
- 接口说明：

接口名称	说明
CreateSDKBuffFromStr	生成水印

接入步骤（Android Studio）

1. 将 sdk/android 文件夹下的内容拷贝到工程目录的 libs 文件夹下:



2. 修改项目的 build.gradle 文件, 设置 jni 文件目录, 添加 jar 依赖:

```
android {
    sourceSets {
        main {
            jniLibs.srcDirs = ['libs/jni'] // 设置 jni 目录
        }
    }
    dependencies {
        implementation files('libs/gamesec.jar') // 添加依赖
    }
}
```

3. Eclipse 接入方法类似, 不需要配置 build.gradle 文件。

接口调用

1. 导入程序包。

```
import com.gamesec.*;
```

2. 实例化 Mark 对象。

```
Mark mark = new Mark();
```

3. 调用 CreateSDKBuffFromStr 生成水印。

```
byte [ ] CreateSDKBuffFromStr (String pSDKinfo, String buffer, String
uDesIp, int uDesPort)
```

● 参数说明:

参数	类型	含义
----	----	----

pSDKInfo	String	水印防护密钥
buffer	String	占位参数，传入空字符串即可
uDesIp	String	服务器 IP，如 “1.2.3.4”
uDesPort	int	服务器端口

- 返回值：

类型	含义
byte[]	计算的水印信息，取20字节

- 调用示例：

```
String pSDKInfo = "566c2dea9420eb37-b6c8-566c2dea9420eb3710525135e8485e80806a2f9c";
String uDesIp = "1xx.xxx.xxx.xxx";
int uDesPort = 8xx9 ;
byte[] bytes = mark.CreateSDKBuffFromStr(pSDKInfo, "", uDesIp, uDesPort);
```

4. 添加水印信息到消息体。代码示例如下：

```
Socket s = new Socket(uDesIp, uDesPort);
OutputStream out = s.getOutputStream();
PrintWriter output = new PrintWriter(out, true);
// 先传入水印信息
output.print(bytes);
output.println("msg msg msg");
BufferedReader input = new BufferedReader(new InputStreamReader(s.getInputStream()));
String msg = input.readLine();
s.close();
```

iOS 接入

预备工作

- 接入 SDK 需要完成以下步骤：

1.1 将 SDK 文件拷贝到工程目录，Swift 工程需要添加桥文件。

1.2 调用 SDK 接口函数，生成水印信息。

1.3 发送报文时，将 20 字节水印信息放在消息体前面。

- SDK 文件包含 a 文件和 h 文件，目录结构如下：

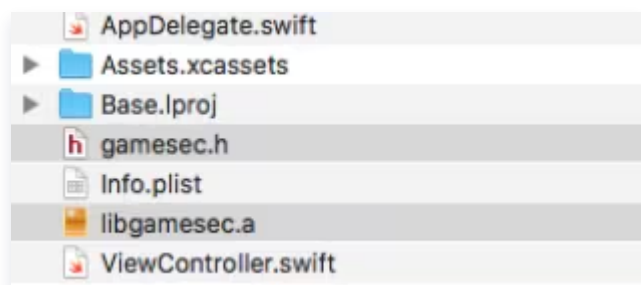


- 接口说明：

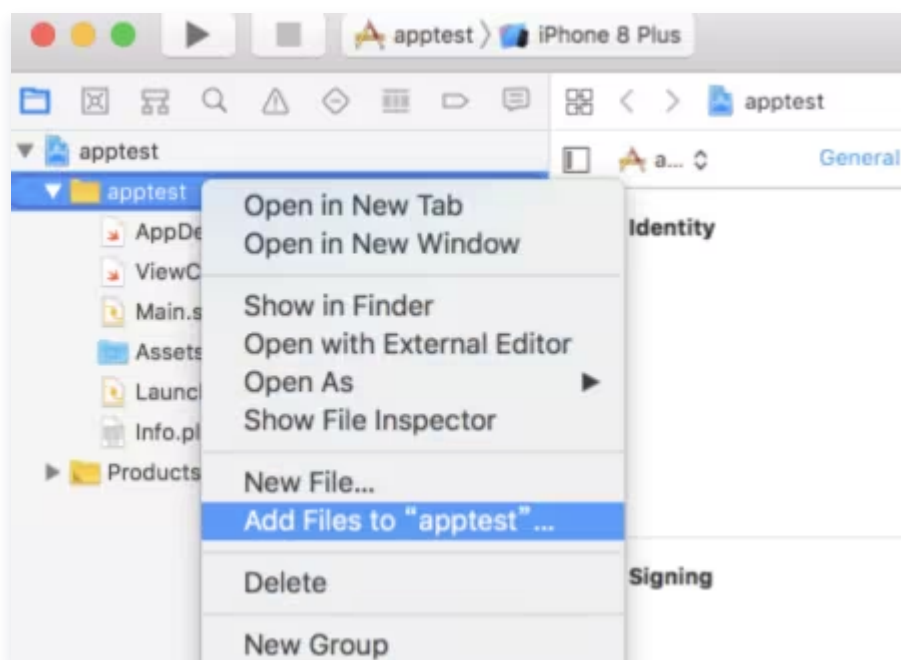
接口名称	说明
CreateSDKBuffFromStr	生成水印

接入步骤（Xcode）

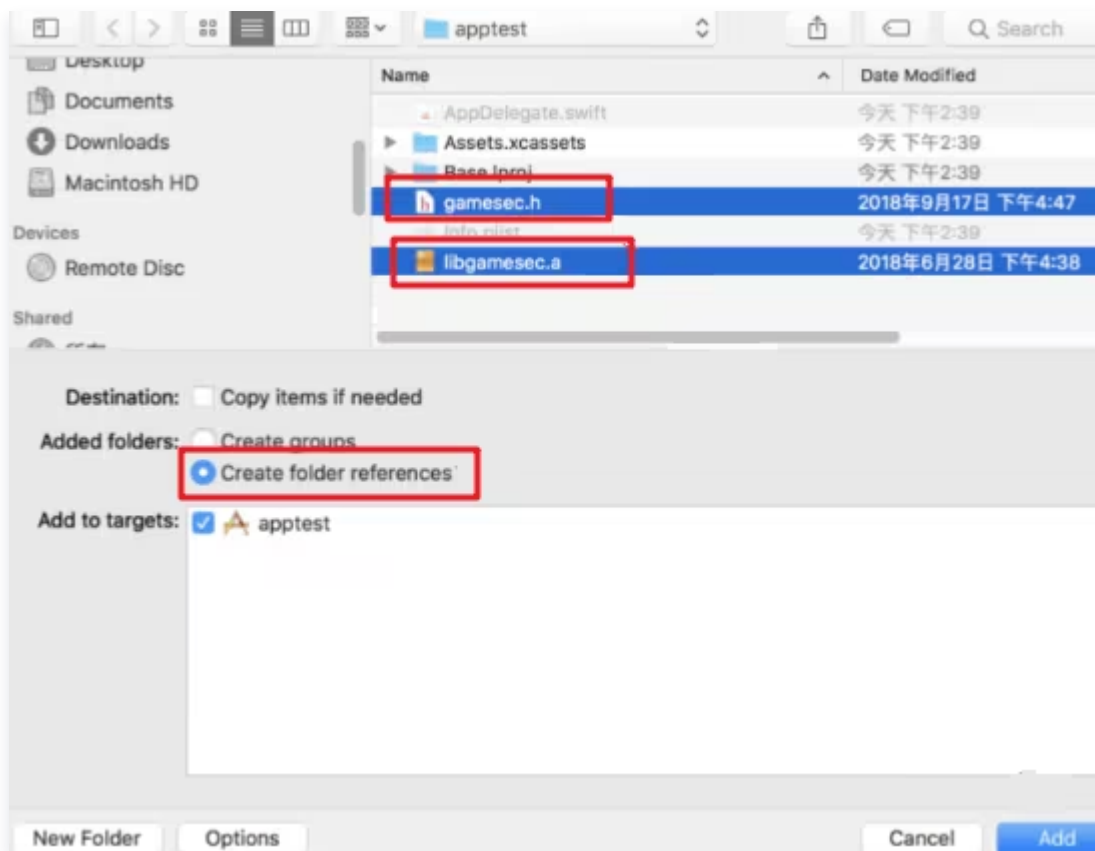
1. 将 sdk/ios 文件夹下的内容拷贝到工程目录：



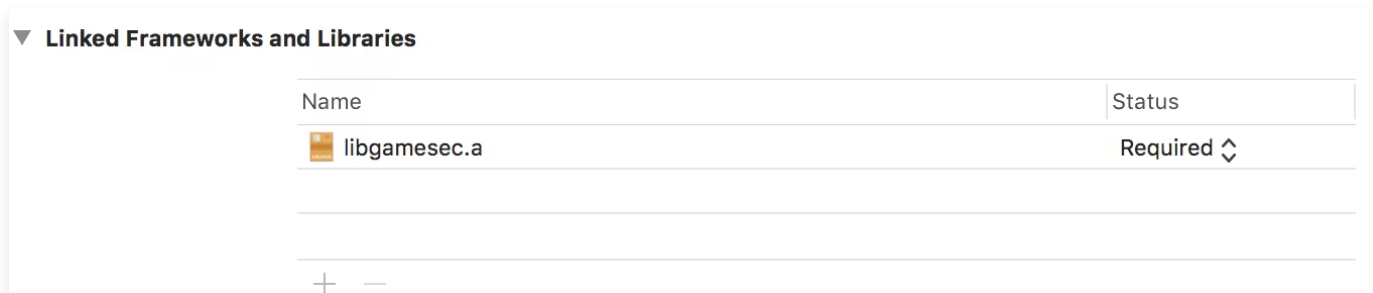
2. 将 SDK 文件添加到 Xcode。右键工程名，单击 “Add Files to”。



3. 在对话框中勾选 “Create folder references”，选中 SDK 的两个文件，单击 **Add**。



4. 左键工程名，选择 General，将 a 文件添加到 “Linked Frameworks and Libraries”：

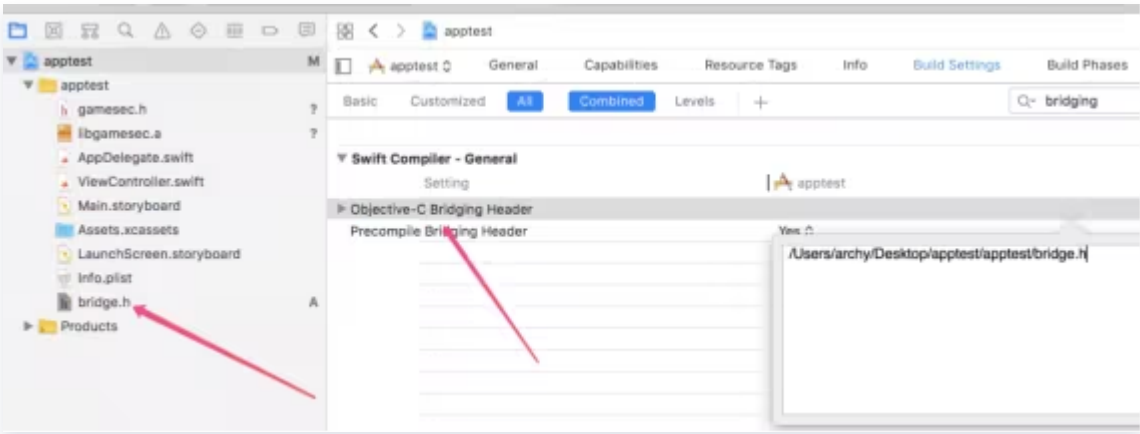


5. 如果是 Swift 项目，需要创建桥文件，Objective-C 项目可以跳过此步骤。创建一个 Header File，命名为 bridge.h。并在文件中添加以下代码：

```
# import "gamesec.h";
```

6. 左键工程名，选择 Build Settings，将 bridge.h 添加到 Objective-C Bridging Header 中：

7.



接口调用

1. Swift 项目可以直接调用生成水印函数，Objective-C 项目需要在使用的文件里面添加头文件：

```
# import "gamesec.h";
```

2. 调用 CreateSDKBuffFromStr 生成水印。

```
uint32_t CreateSDKBuffFromStr(char *pSDKInfo, uint8_t *buffer, char*
uDstIp, uint16_tuDstPort);
```

参数说明：

参数	类型	含义
pSDKInfo	char *	水印防护密钥
buffer	uint8_t *	水印指针，输出水印结果
uDesIp	char *	服务器 IP，如 “1.2.3.4”
uDesPort	uint16_t	服务器端口

 **注意：**
水印结果保存在参数 buffer 中，取20字节。

3. 调用示例。

```
Swift 调用：
let pSDKInfo = UnsafeMutablePointer<Int8>(mutating: (
```



```
"566c2dea9420eb37-b6c8-
566c2dea9420eb3710525135e8485e80806a2f9c"
    as NSString).utf8String);
    var buffer =
UnsafeMutablePointer<UInt8>.allocate(capacity: 20);
    let uDstIp = UnsafeMutablePointer<Int8>(mutating: (
    "115.159.147.198" as NSString).utf8String);
    let uDstport = UInt16.init("8899")!;

    CreateSDKBuffFromStr(pSDKInfo, buffer, uDstIp, uDstport);

    for i in 0 ..< 20 {
        let b = (buffer+i).pointee;
        // 水印信息在前20字节，注意这里输出的是 uint8
        print(" \ (b) ");
    }
```

Object-C 调用:

```
char *pSDKInfo = "566c2dea9420eb37-b6c8-
566c2dea9420eb3710525135e8485e80806a2f9c";
    uint8_t buffer[20];
    char *uDstIp = "115.159.147.198";
    uint16_t uDstPort = 8899;

    CreateSDKBuffFromStr(pSDKInfo, buffer, uDstIp,
uDstPort);

    for(int i=0;i<20;i++)
    {
        // 水印信息在前20字节
        NSLog(@"%d", (int8_t)buffer[i]);
    }
```

4. 发送报文前，添加 20 字节水印信息到消息体前面。

Windows 接入

预备工作

SDK 为 gamesec.dll 文件，有一个生成水印的函数：

```
uint32_t CreateSDKBuffFromStr(char *pSDKInfo, uint8_t *buffer, char*
uDstIp, uint16_t uDstPort);
```

参数说明：

参数	类型	含义
pSDKInfo	char *	水印防护密钥
buffer	uint8_t *	水印指针，输出水印结果
uDesIp	char *	服务器 IP，如 “1.2.3.4”
uDesPort	uint16_t	服务器端口

① 注意：

水印结果保存在参数 buffer 中，取20字节。

接口调用

在使用水印函数时，需先导入 dll 文件，可以使用 LoadLibrary 函数（需要添加 Windows.h ）：

```
// 定义函数指针
typedef int(*FUNC)(char *, uint8_t *, char* , uint16_t );
// 设置 dll 路径
HINSTANCE Hint = ::LoadLibrary(L"E:\\sdk\\gamesec.dll");
FUNC CreateSDKBuffFromStr = (FUNC)GetProcAddress(Hint,
"CreateSDKBuffFromStr");
```

完整调用示例：

```
// 保存水印
uint8_t buffer[BUFFER_SIZE];
memset(buffer, 0, BUFFER_SIZE);

int UDP_TEST_PORT = 8899;

const char * CONST_UDP_SERVER_IP = "115.159.147.198";
char * UDP_SERVER_IP = new char[strlen(CONST_UDP_SERVER_IP)];
strcpy(UDP_SERVER_IP, CONST_UDP_SERVER_IP);
```

```
const char * CONST_pSDKInfo =
"566c2dea9420eb37-b6c8-566c2dea9420eb3710525135e8485e80806a2f9c";
char * pSDKInfo = new char[strlen(CONST_pSDKInfo)];
strcpy(pSDKInfo, CONST_pSDKInfo);

// 调用10次
for (int i = 0; i < 5; i++) {
    CreateSDKBuffFromStr(pSDKInfo, buffer, (char *)UDP_SERVER_IP,
UDP_TEST_PORT);

    for (int i = 0; i <= 20; i++)
    {
        // 水印在前20字节
        printf("%d ", (int8_t)buffer[i]);
    }
    printf("\n\n");
}
```

常见问题

封堵相关问题

最近更新时间：2023-07-21 09:44:44

为什么进行封堵？

腾讯云通过共享基础设施的方式降低用云成本，所有用户共享腾讯云的外网出口。当发生大流量攻击时，除了会影响被攻击对象，整个腾讯云的网路都可能会受到影响。为了避免攻击影响到其他未被攻击的用户，保障整个云平台网络的稳定，需要进行封堵。

为什么不提供免费无限抗攻击？

DDoS 攻击不仅影响受害者，也会对整个云网络造成严重影响，影响云内其它未被攻击的用户。DDoS 防御的成本非常高，一是带宽成本，二是清洗成本。其中最大的成本就是带宽费用，带宽费用以总流量计算，不会考虑是正常流量或是攻击流量而区别收费。

因此，腾讯云在成本可承受的范围内为云服务用户提供免费的 DDoS 基础防护服务，当攻击流量超出免费防护阈值时，腾讯云会屏蔽被攻击 IP 的外网流量。

为什么不能立即解除封堵？

通常 DDoS 攻击会持续一段时间，不会在封堵后立即停止，具体持续时间不定，腾讯云安全团队会根据大数据分析的结果，设定默认封堵时长。

由于封堵是在运营商网路部分生效，被攻击外网 IP 进入封堵后，腾讯云无法监控到攻击流量是否停止。如果在攻击未停止的情况下解除封堵，被攻击外网 IP 将再次进入封堵，同时在解除封堵至再次封堵生效的这段时间内，攻击流量将直接进入腾讯云的基础网路，可能会影响到云内其它客户。另外，封堵是腾讯云向运营商购买的服务，解封次数、频率都有限制。

紧急情况下，通过哪些途径可以提前解封？

- 升级保底容量后，可自动提前解封。
- 使用 DDoS 高防 IP 的用户每天将拥有三次自助解封机会，可在紧急情况下，进行 [自助解封](#)。

为什么自助解封会有次数限制？有哪些限制？

封堵是腾讯云向运营商购买的服务，而运营商有明确的封堵解除时间和频率限制，所以封堵状态无法频繁手动解除。使用 DDoS 高防 IP 的用户每天将拥有三次自助解封机会，当天超过三次后将无法进行解封操作。系统将在每天零点时重置自助解封次数，当天未使用的解封次数不会累计到次日。

怎样预防被封堵？

购买 [DDoS 高防 IP](#) 时，可根据历史攻击流量数据，选择适当的防护峰值，尽可能地确保最大防护峰值大于攻击峰值。

怎样避免解封后再次被封堵？

建议您升级保底防护峰值或弹性防护峰值，提高防御能力。开启弹性防护可帮您抵御大规模流量攻击，且弹性防护按天按量灵活付费，有效节约您的安全成本。

功能相关问题

最近更新时间：2023-07-21 09:44:44

DDoS 高防 IP 支持腾讯云外用户接入防护吗？

支持。DDoS 高防 IP 可以防护任何公网服务器，包括但不限于在腾讯云、其他的云、IDC 机房等。

① 注意：

在中国大陆地区接入的域名必须按照工信部要求进行 ICP 备案。如果域名未备案，将不能提供 DDoS 高防服务。

DDoS 高防 IP 是否支持泛域名？

DDoS 高防 IP 网站业务转发规则配置中，支持对泛域名进行防护。

泛域名解析是指利用通配符（`*`）作为次级域名，以实现所有的次级域名均指向同一 IP。例如，支持配置 `*.tencent.com`。

DDoS 高防 IP 服务是否会自动将回源 IP 地址加入安全组？

不会。用户需手动将回源 IP 段添加至 CVM 安全组中。若用户在源站部署了防火墙或其它主机安全防护软件，也将回源 IP 段添加至相应的白名单中，防止将高防回源 IP 拦截或限速导致业务流量受损。

DDoS 高防 IP 中的源站 IP 可以填写内网 IP 吗？

DDoS 高防 IP 是通过公网进行回源的，不可以直接填写内网 IP。

修改 DDoS 高防 IP 服务的源站 IP 是否有延迟？

修改高防 IP 服务已防护的源站 IP 可秒级生效。

在 DDoS 高防 IP 服务控制台中，更改配置后大约需要多少时间生效？

DDoS 高防 IP 服务中更改配置是秒级生效的。

DDoS 高防 IP 的 IP 回源支持 IPv6 协议吗？

暂时不支持 IPv6 协议。

DDoS 高防 IP 服务是否支持 HTTPS 双向认证？

- 网站接入方式不支持 HTTPS 双向验证。
- 非网站接入且使用 TCP 转发方式时，支持 HTTPS 双向验证。

DDoS 高防 IP 服务是否有抓包文件？

DDoS 高防 IP 服务支持下载抓包文件，具体操作请参考 [查看统计报表](#)。

DDoS 高防 IP 在配置多个源站 IP 时如何负载？

- 网站业务采用默认轮询方式进行负载均衡。
- 非网站业务采用加权轮询方式依次轮流转发。

DDoS 高防 IP 支持转发端口数及支持的域名数分别是多少？

- 转发端口数：TCP/UDP 协议支持转发规则条目总数，默认免费提供60个，支持扩展。
- 支持域名数：HTTP/HTTPS 协议支持转发规则条目总数，默认免费提供60个，支持扩展。

什么是业务带宽，超过之后会有什么影响？

购买的业务带宽是针对整个高防 IP 实例的，指该实例所有正常业务的 IN 或者 OUT 方向的流量。

如果用户的业务流量超过所赠送的规格，将触发流量限速，可能导致随机丢包。若持续出现这种情况，请及时升级更大的业务带宽。

① 说明：

购买 DDoS 高防 IP 服务，默认赠送100M转发业务带宽。

DDoS 高防 IP 服务是否支持会话保持？

DDoS 高防 IP 服务支持会话保持，默认不开启。非网站业务可以通过控制台进行配置操作，请参考 [配置会话保持](#)。

DDoS 高防 IP 服务是否支持健康检查？

非网站业务默认开启健康检查，建议使用默认值，如需要修改，请参考操作步骤 [配置健康检查](#)。

在用户业务绑定 DDoS 高防 IP 后，源站服务器未开启窗口因子 WS 时，访问源站为什么会出现速度慢？

高防服务器默认是开启窗口因子 WS（Window Scaling），若源站服务器未开启，将会导致接收稍大文件数据时，很快把滑动窗口占满出现延迟。建议用户将源站所有服务器开启 WS。关于 WS 的概念及示例说明，可前往腾讯社区 [TCP 速度慢？注意 WS 窗口因子](#) 了解。

计费相关问题

最近更新时间：2023-07-21 09:44:44

高防服务的弹性防护计费模式是否一样？如何计算的？

一样，都是按照当日可防护的攻击流量峰值对应弹性防护峰值区间进行计费，计费详情请参考 [计费概述](#)。

① 说明：

例如，您购买的 DDoS 高防 IP 实例规格是20Gbps保底防护峰值 + 50Gbps弹性防护峰值。如果当天发生 DDoS 攻击事件且最高攻击流量峰值为45Gbps。45Gbps已超过保底防护峰值范围触发弹性防护，且属于40Gbps < 弹性峰值 ≤ 50Gbps计费区间，当天产生弹性费用按照40Gbps < 弹性峰值 ≤ 50Gbps计费区间收取。

如果 DDoS 高防 IP 所防护的 IP 因遭受大流量攻击被封堵，该部分攻击流量是否会列入计费？

DDoS 高防 IP 服务的弹性防护计费规则是针对超出保底防护峰值且小于等于弹性防护峰值的攻击流量进行计费。被封堵即意味着攻击流量已超过所设置的弹性防护峰值，因此超出弹性防护峰值的部分攻击流量不在计费范围内。

购买弹性防护后，如果一个月都没有遭受攻击，是否需要费用？

这种情况下，您只需要支付保底防护的包月费用即可，不产生其它额外的费用。

若购买了100Gbps的保底防护，是否可以降到50Gbps？

不可以。保底防护级别仅支持升级，不支持降级。

业务遭受攻击过程中，是否支持升级弹性防护峰值？

支持。DDoS 高防 IP 服务基础信息界面支持调整弹性防护峰值，支持调升也支持调降。不同地域支持的防护能力不同，弹性防护峰值的具体取值范围请参考 [产品概述](#)。

① 注意：

若当日发生的攻击已经产生计费，修改后次日将以最新的弹性防护峰值进行计费。

受防护的 IP 一天之内遭受多次攻击，是否需要收取多次费用呢？

DDoS 高防 IP 服务是以当日防护的最高攻击流量峰值来计算，只收取一次费用。

如果购买了两个高防服务套餐，且两个高防服务实例遭受的攻击流量都超过保底防护，如何收取弹性防护费用？

弹性防护费用以产品实例为计算单位，如果两个高防服务实例都超过保底防护，则需要分别收取两个高防实例的弹性防护费用。