阿里云
DDoS基础防护

DDoS高防IP

文档版本：20190211

法律声明

阿里云提醒您在阅读或使用本文档之前仔细阅读、充分理解本法律声明各条款的内容。如果您阅读或使用本文档，您的阅读或使用行为将被视为对本声明全部内容的认可。

1. 您应当通过阿里云网站或阿里云提供的其他授权通道下载、获取本文档，且仅能用于自身的合法合规的业务活动。本文档的内容视为阿里云的保密信息，您应当严格遵守保密义务；未经阿里云事先书面同意，您不得向任何第三方披露本手册内容或提供给任何第三方使用。
2. 未经阿里云事先书面许可，任何单位、公司或个人不得擅自摘抄、翻译、复制本文档内容的部分或全部，不得以任何方式或途径进行传播和宣传。
3. 由于产品版本升级、调整或其他原因，本文档内容有可能变更。阿里云保留在没有任何通知或者提示下对本文档的内容进行修改的权利，并在阿里云授权通道中不时发布更新后的用户文档。您应当实时关注用户文档的版本变更并通过阿里云授权渠道下载、获取最新版的用户文档。
4. 本文档仅作为用户使用阿里云产品及服务的参考性指引，阿里云以产品及服务的”现状“、“有缺陷”和“当前功能”的状态提供本文档。阿里云在现有技术的基础上尽最大努力提供相应的介绍及操作指引，但阿里云在此明确声明对本文档内容的准确性、完整性、适用性、可靠性等不作任何明示或暗示的保证。任何单位、公司或个人因为下载、使用或信赖本文档而发生任何差错或经济损失的，阿里云不承担任何法律责任。在任何情况下，阿里云均不对任何间接性、后果性、惩戒性、偶然性、特殊性或刑罚性的损害，包括用户使用或信赖本文档而遭受的利润损失，承担责任（即使阿里云已被告知该等损失的可能性）。
5. 阿里云网站上所有内容，包括但不限于著作、产品、图片、档案、资讯、资料、网站架构、网站画面的安排、网页设计，均由阿里云和/或其关联公司依法拥有其知识产权，包括但不限于商标权、专利权、著作权、商业秘密等。非经阿里云和/或其关联公司书面同意，任何人不得擅自使用、修改、复制、公开传播、改变、散布、发行或公开发表阿里云网站、产品程序或内容。此外，未经阿里云事先书面同意，任何人不得为了任何营销、广告、促销或其他目的使用、公布或复制阿里云的名称（包括但不限于单独为或以组合形式包含”阿里云”、Aliyun”、“万网”等阿里云和/或其关联公司品牌，上述品牌的附属标志及图案或任何类似公司名称、商号、商标、产品或服务名称、域名、图案标示、标志、标识或通过特定描述使第三方能够识别阿里云和/或其关联公司）。
6. 如若发现本文档存在任何错误，请与阿里云取得直接联系。

通用约定

格式	说明	样例
	该类警示信息将导致系统重大变更甚至故障，或者导致人身伤害等结果。	 **禁止:** 重置操作将丢失用户配置数据。
	该类警示信息可能导致系统重大变更甚至故障，或者导致人身伤害等结果。	 **警告:** 重启操作将导致业务中断，恢复业务所需时间约10分钟。
	用于补充说明、最佳实践、窍门等，不是用户必须了解的内容。	 **说明:** 您也可以通过按Ctrl + A选中全部文件。
>	多级菜单递进。	设置 > 网络 > 设置网络类型
粗体	表示按键、菜单、页面名称等UI元素。	单击 **确定**。
`courier` 字体	命令。	执行 `cd /d C:/windows` 命令，进入Windows系统文件夹。
*## *	表示参数、变量。	`bae log list --instanceid` *`Instance_ID`*
[]或者[a|b]	表示可选项，至多选择一个。	`ipconfig` *`[-all|-t]`*
{}或者{a|b}	表示必选项，至多选择一个。	`swich` *`{stand | slave}`*

目录

法律声明.....I
通用约定.....I
1 产品简介..... 1
1.1 什么是DDoS高防IP..... 1
1.2 产品架构.....1
1.3 功能特性.....2
1.4 产品优势.....3
1.5 应用场景.....4
1.6 版本更新.....4
1.6.1 高防IP V8.5.2版本发布.....4
1.6.2 高防IP V8.5版本发布..... 7
1.6.3 高防IP V8.6.7新版本发布.....7
1.6.4 高防IP V8.6.5新版本发布.....8
2 产品定价.....10
2.1 购买DDoS高防IP实例..... 10
2.2 线路购买指南.....12
2.3 计费方式.....16
2.4 续费流程.....17
2.5 欠费说明.....18
2.6 高防IP退款.....18
2.7 升级高防IP实例规格.....19
2.8 降配高防IP实例规格.....21
2.9 防护能力增长规格说明.....23
3 快速入门.....24
3.1 防护网站业务.....24
3.1.1 概述.....24
3.1.2 启用高防实例.....24
3.1.3 步骤1：HTTP网站接入..... 25
3.1.4 （可选）步骤1：HTTPS网站接入.....26
3.1.5 步骤2：放行回源IP段.....28
3.1.6 步骤3：验证配置生效..... 29
3.1.7 步骤4：修改DNS解析.....29
3.2 防护非网站业务.....31
3.2.1 概述.....31
3.2.2 步骤1：配置四层转发..... 32
3.2.3 步骤2：放行回源IP段.....33
3.2.4 步骤3：验证配置生效..... 34
3.2.5 （可选）步骤4：修改DNS解析.....35
4 用户指南.....37

4.1 业务接入配置.....37
4.1.1 网站业务CNAME方式接入配置.....37
4.1.2 非网站业务CNAME方式接入配置.....38
4.1.3 CNAME接入状态说明.....39
4.1.4 CNAME自动调度.....40
4.1.5 修改业务源站IP.....41
4.1.6 修改网站业务高防线路和源站配置.....42
4.1.7 高防线路默认解析说明.....45
4.2 网络七层防护设置.....46
4.2.1 HTTP(S) Flood攻击防护设置.....46
4.2.2 黑白名单设置.....48
4.2.3 流量调度方式管理.....49
4.2.4 黑洞解封.....53
4.2.5 流量封禁.....54
4.3 网络四层防护设置.....55
4.3.1 四层清洗模式设置.....55
4.3.2 非网站业务健康检查配置.....58
4.3.3 非网站业务DDoS防护策略配置.....59
4.3.4 非网站业务会话保持配置.....60
4.4 实例管理.....61
4.4.1 启用停用某条线路.....61
4.4.2 调整弹性防护带宽.....62
4.4.3 更换 ECS IP.....63
4.4.4 管理抗D包.....64
4.5 统计报表.....66
4.5.1 查看安全概览报表.....66
4.5.2 查看安全报表.....76
4.5.3 查看业务遭受的攻击情况.....77
4.5.4 配置DDoS事件告警通知.....80
4.6 日志查询.....81
4.6.1 操作日志.....81
4.6.2 全量日志.....82
4.7 安全服务.....85
4.7.1 开通高防安全服务授权.....85
4.7.2 查看安全专家操作日志.....87
4.7.3 取消高防安全服务授权.....88
4.8 安全专家指导服务.....90
5 最佳实践.....92
5.1 DDoS高防接入配置最佳实践.....92
5.2 设置DDoS高防IP的自定义告警规则.....101
5.3 查看DDoS高防IP的实时监控数据.....102
5.4 多线路高防实例回源到不同源站的配置方法.....104
5.5 云外主机获取真实客户端源IP.....106
5.6 “高防IP+阿里云CDN”同时接入.....108
5.7 "高防IP+云盾WAF"同时使用.....108

5.8 如何通过高防IP判断遭受的攻击类型..... 110
5.9 如何将已配置高防的业务切换至其他高防实例.....110
5.10 源站IP暴露的解决办法..... 111
5.11 获取客户端真实IP..... 112
5.12 高防源站保护..... 119
6 API参考..... 122
7 常见问题.....123
7.1 BGP高防是什么？有什么优势？.....123
7.2 配置高防后访问网站，提示502错误..... 124
7.3 高防IP常见问题.....126
7.4 高防IP卡顿、延迟、访问不通等问题排查..... 133
7.5 配置高防后访问网站提示504错误..... 140
7.6 如何查看高防回源IP段..... 140
7.7 弹性计费常见问题..... 141
7.8 配置高防后网站上传大文件失败..... 143
7.9 高防IP与安全组规则设置问题..... 143
7.10 SNI可能引发的HTTPS访问异常.....144
7.11 HTTPS证书转换成PEM格式..... 146
7.12 HTTPS业务异常状态说明..... 147
7.13 香港高防备用IP使用说明..... 147
7.14 访问高防端口不通排查.....148
7.15 高防IP是否需要网站备案接入..... 149
7.16 上传HTTPS证书出现“参数错误”解决办法..... 150
7.17 配置高防后业务访问报502错误..... 150
7.18 高防告警短信配置.....151
7.19 配置高防后访问业务缓慢.....151
7.20 配置高防后通过http和https上传大文件失败.....152
7.21 如何跨账户配置高防.....153
7.22 配置高防后系统建立连接慢.....153
7.23 GET请求返回的HTTP状态为413错误..... 154
7.24 配置高防IP后无法Ping通..... 155
7.25 NTP服务的DDoS攻击.....155
7.26 配置高防后不能实现会话保持的排查思路.....156
7.27 如何判断DDoS高防IP的攻击类型..... 157
7.28 HTTP报文经过Web应用防火墙后响应头没有Content-Length.....158
7.29 网站防护和非网站防护的区别.....159
7.30 健康检查主动探测IP..... 160

1 产品简介

1.1 什么是DDoS高防IP

云盾DDoS高防IP产品是针对互联网服务器（包括非阿里云主机）在遭受大流量的DDoS攻击后导致服务不可用的情况，推出的付费增值服务。您可以通过配置DDoS高防IP，将攻击流量引流到高防IP，确保源站的稳定可靠。

DDoS攻击防护峰值带宽 20 Gbps ~ 600 Gbps，最低￥16,800 / 月（20G）。同时，提供按天弹性付费方案，按当天攻击规模灵活付费。

您购买DDoS高防IP服务后，把域名解析到高防IP（Web业务把域名解析指向高防IP；非Web业务，把业务IP替换成高防IP），并配置源站IP。所有公网流量都经过高防IP机房，通过端口协议转发的方式将访问流量通过高防IP转发到源站IP，同时将恶意攻击流量在高防IP上进行清洗过滤后将正常流量返回给源站IP，从而确保源站IP稳定访问。

配置DDoS高防IP服务后，当您遭受DDoS攻击时，无需额外做流量牵引和回注。

1.2 产品架构

DDoS高防IP服务使用专门的高防机房提供DDoS防护服务，通过引流、清洗、回注的方式将正常业务流量转发至源站服务器，确保源站服务器的稳定可用。

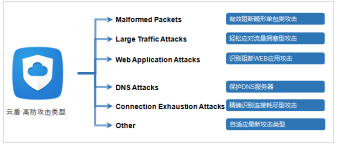
阿里巴巴集团云盾产品所涉及的产品组件，全部为自主研发产品，拥有充分自主知识产权。

从引流技术上，DDoS高防IP服务支持BGP与DNS两种方案。防护的方式采用被动清洗方式为主、主动压制为辅的方式，对攻击进行综合运营托管，保障用户可在攻击下高枕无忧。

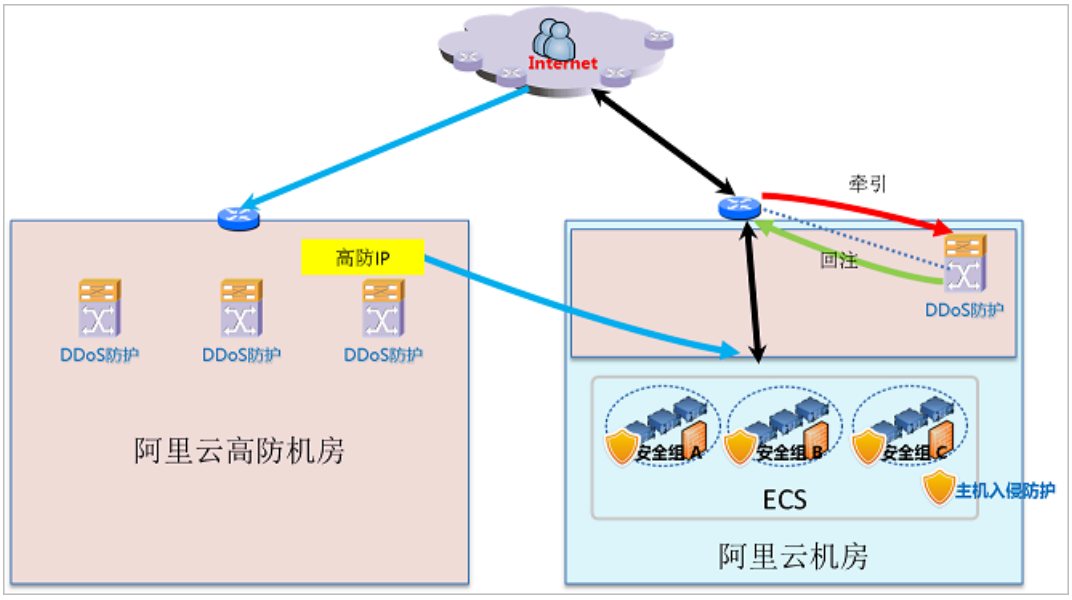
针对攻击在传统的代理、探测、反弹、认证、黑白名单、报文合规等标准技术的基础上，结合Web安全过滤、信誉、七层应用分析、用户行为分析、特征学习、防护对抗等多种技术，对威胁进行阻断过滤，保证被防护用户在攻击持续状态下，仍可对外提供业务服务。

当前，阿里云建设的防护系统，防护能力已高达T级，并且不断在各地扩容防护能力节点。

阿里云基于自主研发的云盾产品，为您提供DDoS防护服务，可以防护SYN Flood、UDP Flood、ACK Flood、ICMP Flood、DNS Query Flood、NTP reply Flood、CC攻击等三到七层DDoS攻击，可防护的攻击类型请参考下图：

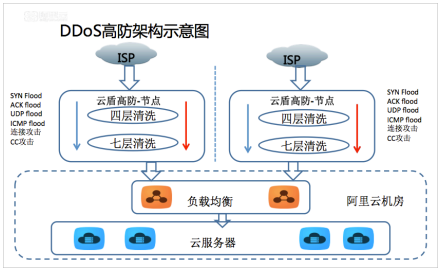


DDoS高防IP服务使用专门的高防机房为您提供DDoS防护服务。网络拓扑示意图如下：



左侧是DDoS高防IP防护服务结构，右侧是阿里云提供的*DDoS*基础防护服务结构。

您购买DDoS高防IP之后，把域名解析到高防IP（Web业务把域名解析指向高防IP；非Web业务把业务IP换成高防IP），同时在DDoS高防IP上设置转发规则。所有的公网流量都会先经过高防机房，通过端口协议转发的方式将访问流量通过高防IP转发到源站IP，同时将恶意攻击流量在高防IP上进行清洗过滤后将正常流量返回给源站IP，从而确保源站IP稳定访问的防护服务。



1.3 功能特性

云盾DDoS高防IP拥有东半球最大的高防中心，帮助您轻松应对大流量攻击，确保云服务稳定正常。

功能	子功能	描述
攻击防护类型	畸形报文过滤	过滤frag flood，smurf，stream flood，land flood攻击。
攻击防护类型	畸形报文过滤	过滤IP畸形包、TCP畸形包、UDP畸形包。
攻击防护类型	传输层DDoS攻击防护	过滤Syn flood，Ack flood，UDP flood，ICMP flood，Rstflood。

功能	子功能	描述
攻击防护类型	Web应用DDoS攻击防护	过滤HTTP Get flood，HTTP Post flood，高频攻击等攻击，支持HTTP特征过滤、URI过滤、host过滤。

特性

- 防护多种DDoS类型攻击

  包括但不限于以下攻击类型：ICMP Flood、UDP Flood、TCP Flood、SYN Flood、ACK Flood 攻击。
- 随时更换防护IP

  可随时更换防护的IP，让您配置更自由、防护更安全。
- 弹性防护

  DDoS防护阈值弹性调整，您可以随时升级到更高级别的防护，整个过程服务无中断。
- 精准防护报表

  提供实时精准的流量报表及攻击详情信息，让您及时、准确获得当前服务详情。

1.4 产品优势

云盾DDoS高防IP帮助您防护海量DDoS攻击，具备精准、弹性、高可靠、高可用等优势。

- 防护海量DDoS攻击

  成功防御大于1Tbps的DDoS攻击。

  有效抵御所有各类基于网络层、传输层及应用层的DDoS攻击。
- 精准攻击防护

  针对交易类、加密类、七层应用、智能终端、在线业务攻击等实现精准防护，使得威胁无处可逃。
- 隐藏用户服务资源

  云盾DDoS高防IP服务可对用户站点进行更换并隐藏。使用云盾资源作为源站的前置，使攻击者无法找到受害者网络资源，增加源站安全性。
- 弹性防护

  DDoS防护性能支持弹性调整。您可在管理控制台自助升级，秒级生效，且无需新增任何物理设备。同时，业务上也无需进行任何调整，整个过程服务无中断。
- 高可靠、高可用的服务

  全自动检测和攻击策略匹配，实时防护，清洗服务可用性99.99%。

1.5 应用场景

云盾高防IP，服务于阿里云以及阿里云外所有客户。

使用场景

云盾高防IP服务的主要使用场景包括，金融、娱乐（游戏）、媒资、电商、政府等网络安全攻击防护场景。

建议如下对用户业务体验实时性要求较高的业务，接入高防IP进行防护，包括：实时对战游戏、页游、在线金融、电商、在线教育、O2O等。

1.6 版本更新

1.6.1 高防IP V8.5.2版本发布

高防IP V8.5.2版本发布于2017年7月6日。

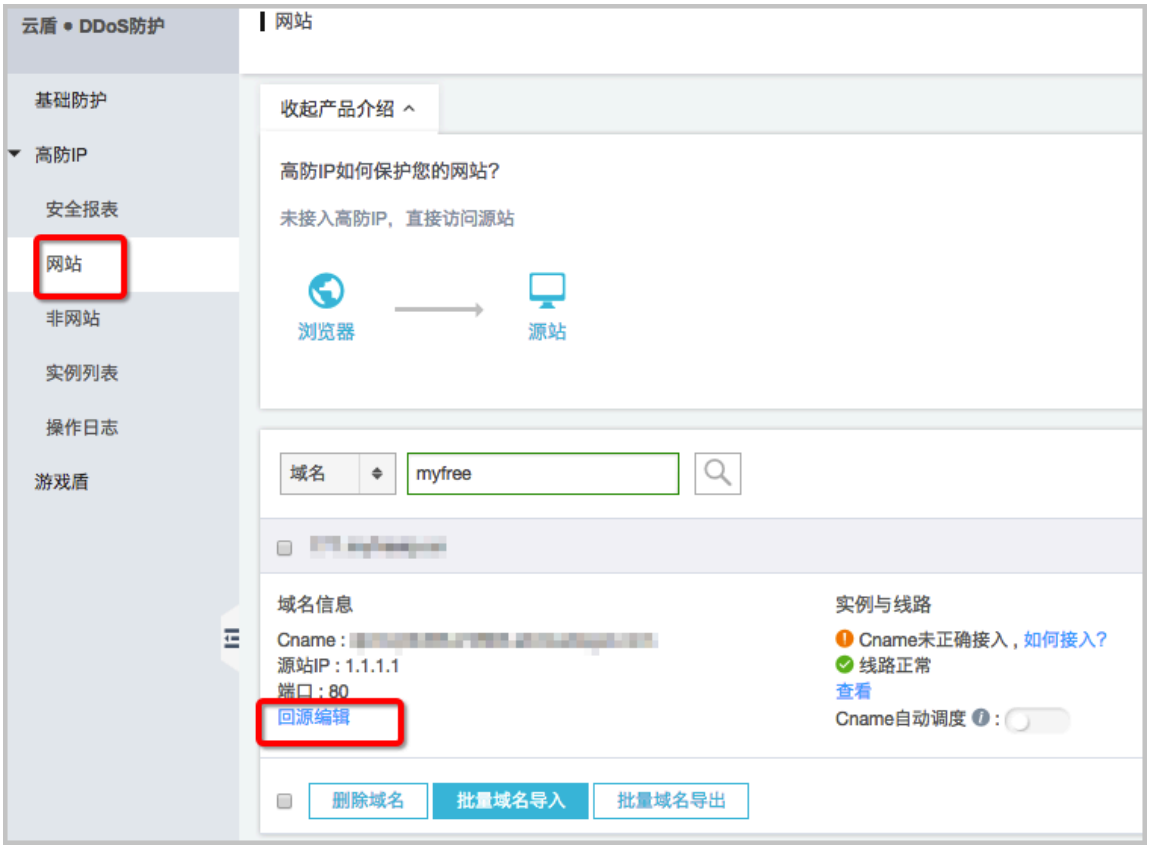
更新内容

- 网站防护
  - 优化回源编辑页面。
  - 优化线路状态错误提示信息。
  - 新增IP维度域名查询。
  - 优化域名修改后页面刷新体验。
  - CC自定义封禁时间由秒钟调整为分钟。
- 高危操作增加二次弹框确认，例如CNAME开关、域名解析开关等。
- 修复域名批量导出超时问题。

主要更新页面

- DDoS防护 > 高防IP > 网站 > 回源编辑页面

  1. 打开回源编辑页面。



2. 在回源编辑页面中，可以选择停止或者启用当前高防IP的解析。当停止某条高防线路IP的解析时，域名解析将停止该线路的解析。

3. 在回源编辑页面中，单击编辑源站，可以选择回源到IP或者回源到CNAME。

   典型应用场景：高防IP回源到WAF时，回源可以选择源站域名模式。

4. 在回源编辑页面中，单击编辑线路，可以选择当前域名使用哪些高防IP。一般情况下，默认选择一组实例里的电信、联通、BGP三个IP即可。

   单击停用，可以停止使用某个高防IP。

- DDoS防护 > 高防IP > 网站 > 线路状态，优化错误提示信息。

- DDoS防护 > 高防IP > 网站页面，新增通过高防IP查询域名功能。

  支持查询一个高防IP已绑定的域名情况。

1.6.2 高防IP V8.5版本发布

介绍了高防IP V8.5版本的更新说明。

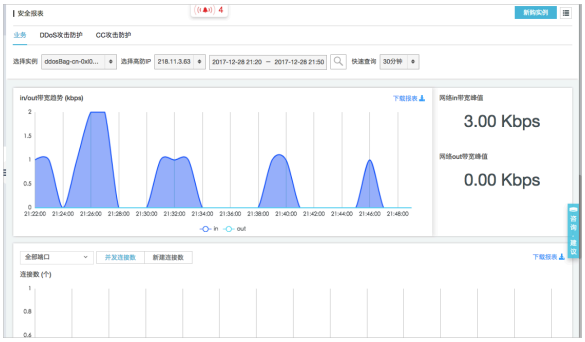
详细更新说明请参考云盾高防升级说明v8.5版本。

- 优化配置流程，增强防护功能，开放CC防护自定义配置。
- 合并电信、联通、BGP配置。
- 开放CC频率检测功能。
- 开放域名解析调整功能，支持一键停止某条线路解析。

1.6.3 高防IP V8.6.7新版本发布

高防IPIP V8.6.7版本发布，开放用户业务IN/OUT带宽查询，开放新建连接、并发连接数据查询。

- 高防IP支持IN/OUT带宽查询



  - IN：网络接收流量，包含正常访问流量和恶意攻击流量
  - OUT：业务出流量，源站业务响应正常访问的出流量
- 高防IP支持新建、并发连接查询

> 说明:
> 新建、并发连接数据可以基于不同协议不同端口查询

- IN/OUT流量、新建连接、并发连接数据可以下载，支持7天以内数据查询和下载。

> 说明:
> 新建连接取的是一段时间内的平均值，当平均值小于1的时候，取整后可能导致计算结果为0。

1.6.4 高防IP V8.6.5新版本发布

高防IP V8.6.5版本发布，大幅增强网站接入能力。

主要优化内容：

- 网站接入协议支持websocket。
- 网站接入时可以和证书管理中心打通，不用频繁上传证书，可以直接选取证书管理中心中已经上传好的证书。

WS是Web Socket的缩写，WebSocket是HTML5一种新的协议。它实现了浏览器与服务器全双工通信，能更好地节省服务器资源和带宽并达到实时通讯。WebSocket建立在TCP之上，同HTTP一样通过TCP来传输数据，但是它和HTTP最大不同是：

WebSocket是一种双向通信协议，在建立连接后，WebSocket服务器和Browser/Client Agent都能主动的向对方发送或接收数据，就像Socket一样；WebSocket需要类似TCP的客户端和服务器端通过握手连接，连接成功后才能相互通信。

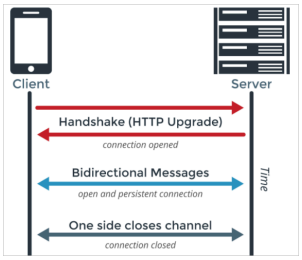
WSS是Web Socket Secure的缩写即WebSocket加密版本。

为何使用WS/WSS?

随着互联网的蓬勃发展，各种类型的Web应用层出不穷，很多应用要求服务端有能力进行实时推送能力（比如直播间聊天室），以往很多网站为了实现推送技术，所用的技术都是轮询。轮询是在特定的的时间间隔（如每1秒），由浏览器对服务器发出HTTP请求，然后由服务器返回最新的数据给客户端的浏览器。这种传统的模式带来很明显的缺点，即浏览器需要不断地向服务器发出请求，然而HTTP请求可能包含较长的头部，其中真正有效的数据可能只是很小的一部分，显然这样会浪费很多的带宽资源。

在这种情况下，HTML5定义了WebSocket协议，能更好地节省服务器资源和带宽，并且能够更实时地进行通讯。WebSocket实现了浏览器与服务器全双工(full-duplex)通信，允许服务器主动发送信息给客户端。

WebSocket协议的交互过程如下图所示。



如何在高防IP上启用WS/WSS支持?

方法：高防IP > 网站 > 添加域名，启用ws。如果是wss，需要上传证书。

证书上传优化

新版本优化了证书上传逻辑，用户在证书管理中心上传证书后，高防页面可以直接选用 已经上传过的证书

- 

2 产品定价

2.1 购买DDoS高防IP实例

根据您的业务安全需求，选择购买适合的DDoS高防IP实例套餐。

背景信息

> **说明:**
>
> - 购买高防IP服务，您需完成实名认证。
> - DDoS高防IP实例仅适用于业务服务器部署在中国大陆地域内的DDoS防护场景。如果您需要防护的业务服务器是部署在中国大陆以外的地域，请选择*DDoS*高防（国际）。

操作步骤

1. 登录阿里云*DDoS*高防*IP*购买页面。

   > **说明:**
   > 建议您选购网络质量和稳定性更优的新BGP高防IP服务。

2. 根据您的业务需要选择线路、保底防护带宽、弹性防护带宽、端口数、业务带宽。

   - 线路：指高防IP实例所包含的IP的线路。关于线路的详细说明，请查看高防IP线路说明。

     > **说明：**
     > 如果您对线路质量有较高要求或者需要20G以上保底防护带宽的BGP线路高防IP服务，建议您购买新BGP高防IP服务。关于新BGP高防IP服务的详细说明，请查看什么是新BGP高防IP。

   - 保底防护带宽：指高防IP实例的保底防护带宽。根据所选择的保底防护带宽及购买时长，生成预付费账单。

- 弹性防护带宽：指高防IP实例的最高弹性防护带宽。对于超出保底防护带宽的攻击进行弹性防护，并根据当时实际发生的超出保底防护带宽攻击峰值生成后付费账单。

  说明：

  如果您不需要启用弹性防护能力，只需将弹性防护带宽的值设置为与保底防护带宽的值一致即可，高防IP实例将不会产生任何后付费防护费用且该实例的最高防护带宽为保底防护带宽值。

- 端口数：指高防IP实例支持的最大转发端口数量，即通过TCP/UDP协议转发支持的最大条目数。
- 业务带宽：指非DDoS攻击状态下高防IP实例所支持的正常业务消耗带宽。

3. 选择您需要的套餐后，单击立即购买，进行付费，完成购买流程。

   更多信息：

   - 高防IP服务计费方式
   - 弹性计费常见问题

2.2 线路购买指南

高防IP目前主要支持五种高防线路套餐。

- 电信+联通+BGP线路
- 电信+联通+移动线路
- 电信+联通线路
- BGP线路
- 新BGP高防IP（推荐需要大于20G的BGP线路保底防护带宽的用户购买）

说明：

以上五种高防线路仅适用于业务服务器部署在中国大陆地域内的DDoS防护场景。如果您需要防护的业务服务器是部署在中国大陆以外的地域，选择DDoS高防（国际）。

线路名称	保底防护带宽	弹性防护带宽	典型购买场景推荐
电信+联通+BGP(推荐购买)	20Gbps (每条线路)	电信、联通最高300Gbps BGP最高100Gbps(最高清洗能力根据网络流量实时动态调整，有时会低于100Gbps)	满足电信、联通和其它运营商（如移动、教育网、铁通、长城宽带等）线路高速访问需求。启用负载均衡流量调度方式（默认流量调度方式），BGP线路遭遇大于20G的攻击流量被黑洞后会自动把解析切换到电信线路，BGP线路业务访问恢复时间根据DNS的缓存生效时间而定，一般10分钟左右。如果想同时兼顾各类运营商高速接入访问以及大流量攻击防护，推荐使用新BGP高防IP。
电信+联通+移动	20Gbps-300Gbps（每条线路）	电信、联通最高300Gbps,移动150Gbps	可满足电信、联通和移动三线访问业务大流量攻击防护需求。
电信+联通	20Gbps-300Gbps（每条线路）	电信、联通最高300Gbps	可满足电信和联通单／双线访问业务大流量攻击防护需求。
BGP	20Gbps	BGP最高100Gbps(最高清洗能力根据网络流量实时动态调整，有时会低于100Gbps)	可同时满足电信、联通和其它运营商（如移动、教育网、铁通、长城宽带等）线路访问业务和100G以内大流量攻击防护需求（保底带宽最高20G，弹性防护带宽最高100G）。如需更高BGP保底防护带宽，推荐使用新BGP高防IP。

线路名称	保底防护带宽	弹性防护带宽	典型购买场景推荐
新BGP高防IP	30Gbps-600Gbps	600Gbps（支持定制更高的弹性防护带宽）	非网站类业务大流量防护且需要覆盖中国大陆地域的主流运营商用户高速接入，优先推荐使用新BGP高防IP · 网站类低并发业务（如正常业务每秒几千QPS）优先推荐选购新BGP高防IP · 网站类高并发业务（如正常业务每秒数万以上的QPS）建议选购电信+联通+BGP或其它多线高防IP

关于弹性防护带宽

弹性防护带宽可设置为大于或等于保底带宽，如果弹性防护带宽等于保底带宽，意味着当前最高防护带宽就是保底带宽值，这样不会产生后付费；如果弹性带宽设置为大于保底带宽，则当前最高防护带宽值为弹性带宽值，遇到大于保底带宽或保底带宽具备的CC防护能力但小于弹性防护带宽或弹性防护带宽具备的CC防护能力的攻击时，能够进行有效防护，但是会产生后付费。

后付费收费详情请点击查看。

可以在第一次下单购买DDoS高防IP的页面就选定弹性带宽值或者在控制台上根据自身流量情况进行自行调整。

> **说明:**
> 调整前请仔细了解后付费收费详情。

弹性防护（按天后付费）

DDoS攻击防御峰值	CC攻击防御峰值	弹性防护费用（天），电信、联通、移动线路	弹性防护费用（天），香港、新加坡、德国、美东线路	弹性防护费用（天），BGP线路
20 Gb<攻击峰值≤30 Gb	60,000 QPS<攻击峰值≤100,000 QPS	1,787	2,900	3,880
30 Gb<攻击峰值≤40 Gb	100,000 QPS<攻击峰值≤130,000 QPS	3,120	4,900	4,880
40 Gb<攻击峰值≤50 Gb	130,000 QPS<攻击峰值≤160,000 QPS	4,453	6,900	8,800
50 Gb<攻击峰值≤60 Gb	160,000 QPS<攻击峰值≤200,000 QPS	5,787	9,000	12,800
60 Gb<攻击峰值≤70 Gb	200,000 QPS<攻击峰值≤230,000 QPS	9,120	14,100	15,680
70 Gb<攻击峰值≤80Gb	230,000 QPS<攻击峰值≤260,000 QPS	11,120	17,200	19,680
80Gb<攻击峰值≤100Gb	260,000 QPS<攻击峰值≤300,000 QPS	13,120	20,300	23,680
100Gb<攻击峰值≤150Gb	300,000 QPS<攻击峰值≤450,000 QPS	16,453	25,400	-
150Gb<攻击峰值≤200Gb	450,000 QPS<攻击峰值≤600,000 QPS	19,120	29,400	-
200Gb<攻击峰值≤300Gb	600,000 QPS<攻击峰值≤1,000,000 QPS	24,453	-	-
300Gb<攻击峰值≤400Gb	1,000,000 QPS<攻击峰值≤1,500,000 QPS	40,000	-	-
400Gb<攻击峰值≤500Gb	1,500,000 QPS<攻击峰值≤2,000,000 QPS	50,000	-	-
500Gb<攻击峰值≤600Gb	2,000,000 QPS<攻击峰值≤2,500,000 QPS	60,000	-	-

电信+联通+BGP（推荐）

购买此线路后， 将获得三个高防IP，分别对应电信、联通和BGP线路。每条线路具备20Gbps的保底防护带宽，电信、联通线路的两个IP具备弹性防护能力，最大防护带宽300Gbps。BGP线路也具备弹性防护能力，BGP线路最大防护带宽根据当前网络流量情况在20Gbps-100Gbps这个区间进行实时动态调整。

BGP线路的实用价值在于连接不同运营商，提供无需跨网的丝滑接入体验。更多关于BGP高防的介绍，请查看*BGP*高防是什么？有什么优势。

购买并启用该DDoS高防IP线路后，建议将三个IP配置同样的转发规则，以达到最大的防护能力和最好的访问体验。

说明:

网站类业务如使用电信、联通线路，网站域名需要在工信部进行ICP备案；如使用BGP线路，除网站域名需要在工信部备案之外，还需要在阿里云进行备案或者接入。

电信+联通+移动

购买此线路后，将获得三个高防IP，分别对应电信、联通和移动线路，电信和联通具备最大300Gbps的弹性防护能力，移动具备最大150Gbps的弹性防护能力。

说明:

- 网站类业务使用电信、联通和移动线路，网站域名需要在工信部进行ICP备案。
- 使用三线高防，部分用户通过其它运营商（如教育、铁通或长城宽带）访问网站时，因为需要跨网，可能会出现丢包或延迟现象。针对这个问题，建议使用*BGP*线路解决。

电信+联通

购买此线路后，将获得两个高防IP，分别对应电信和联通线路，都具备最大300Gbps的弹性防护能力。

说明:

- 网站类业务使用电信、联通线路，网站域名需要在工信部进行ICP备案。
- 使用双线高防，部分用户通过其它运营商（如移动、教育、铁通或长城宽带）访问网站时，因为需要跨网，可能会出现丢包或延迟现象。针对这个问题，建议使用*BGP线路*解决。

BGP线路

购买此线路后，将获得一个BGP高防IP，基础防护带宽有10G和20G两种规格。

由于，遭受的DDoS攻击超过基础防护带宽后会进入黑洞，建议攻击流量不大（100G以下）的用户使用。

说明:

使用BGP线路，除网站域名需要在工信部备案之外，还需要在阿里云进行备案或者接入。

新BGP高防IP线路

购买此线路后，无需启用即可使用，一个IP覆盖中国大陆地域主流运营商用户的高速接入。
新BGP高防线路除了现有BGP线路的优势外， 关键突破了现有BGP防护带宽能力，由现有的百G防护能力跃升到T级防护能力。更多关于新BGP高防的详细介绍，查看*新BGP高防IP产品详情*。

说明:

网站类业务需要在工信部进行ICP备案，还需要在阿里云进行备案或者接入。

2.3 计费方式

DDoS高防IP采用“预付费+后付费”的混合计费模式。其中，基础防护带宽部分以预付费方式进行计费，弹性防护部分按实际发生的攻击峰值计算生成后付费账单。

计费说明

计费模式： 混合计费模式

计费单位：人民币（RMB）

计费项：基础防护 + 弹性防护

付费方式：预付费 + 后付费

计费周期：基础防护带宽（单位：Gbps）和 CC 防护能力（单位：QPS）按月/年计费。购买时，生成预付费订单进行付费。

扣费周期：弹性防护带宽（单位：Gbps）和 CC 防护能力（单位：QPS）按日计费。按照前一日实际发生的DDoS攻击峰值或CC攻击峰值取较大的计费区间计算，生成后付费账单。

到期说明

- 服务距离到期时间前的七、三、一 天，会通过短信/邮件的形式提醒您服务即将到期，并提醒您续费。
- 如到期后没有续费，DDoS防护会恢复到默认的免费防护能力。
- 服务到期后您的 DDoS 高防相关配置为您保留七天。七天内完成续费，则可继续使用原高防防护服务；七天后，高防 IP 自动释放，服务将不可用。

欠费说明

- 欠费：当您的帐号余额不满防护上限一天的费用时，将会通过短信通知您，账户余额不足，并自动关闭弹性防护按量付费模式，防御能力下调到基础防护。
- 结清：当您将已产生的弹性防护费用结清后，弹性防护能力将自动恢复至欠费前所设置的弹性防护带宽。

产品定价

关于DDoS高防IP服务的详细价格信息，请前往阿里云*DDoS*高防*IP*定价页面查看。

变更计费方式与变更配置

您可以随时进行续费、或升级的操作。

- 续费：您充值续费后，可以选择延长高防 IP 服务的周期。
- 升级：您可以选择升级基础防护的防护能力。

  例如，您可以从 20Gbps/60,000QPS 升级到 300 Gbps/1,000,000QPS 的基础防护能力。

  > 说明:
  > 部分线路无法升级到 300Gbps/1,000,000QPS 的防御能力，最高可升级配置以实际线路为准。

2.4 续费流程

您可以在DDoS高防管理控制台中，进行高防IP服务的续费。

操作步骤

1. 登录到 云盾管理控制台。
2. 定位到DDoS高防IP > 高防IP > 示例列表，单击目标实例下的续费。
3. 在续费页面选择续费时长，并完成相应支付流程。

2.5 欠费说明

高防IP服务到期三天前，您将收到短信或邮件提醒，告知您服务即将到期，并提醒您续费。

服务到期

当您购买的防护服务到期后，高防IP服务将停止。如您在服务到期后没有续费，DDoS防护将恢复到免费的5G防护能力。

到期配置

当您购买的防护服务到期后，高防IP相关配置将为您保留七天。如七天内完成续费，原高防IP继续为您提供防护；七天后，您之前使用的高防IP释放，服务不可用。

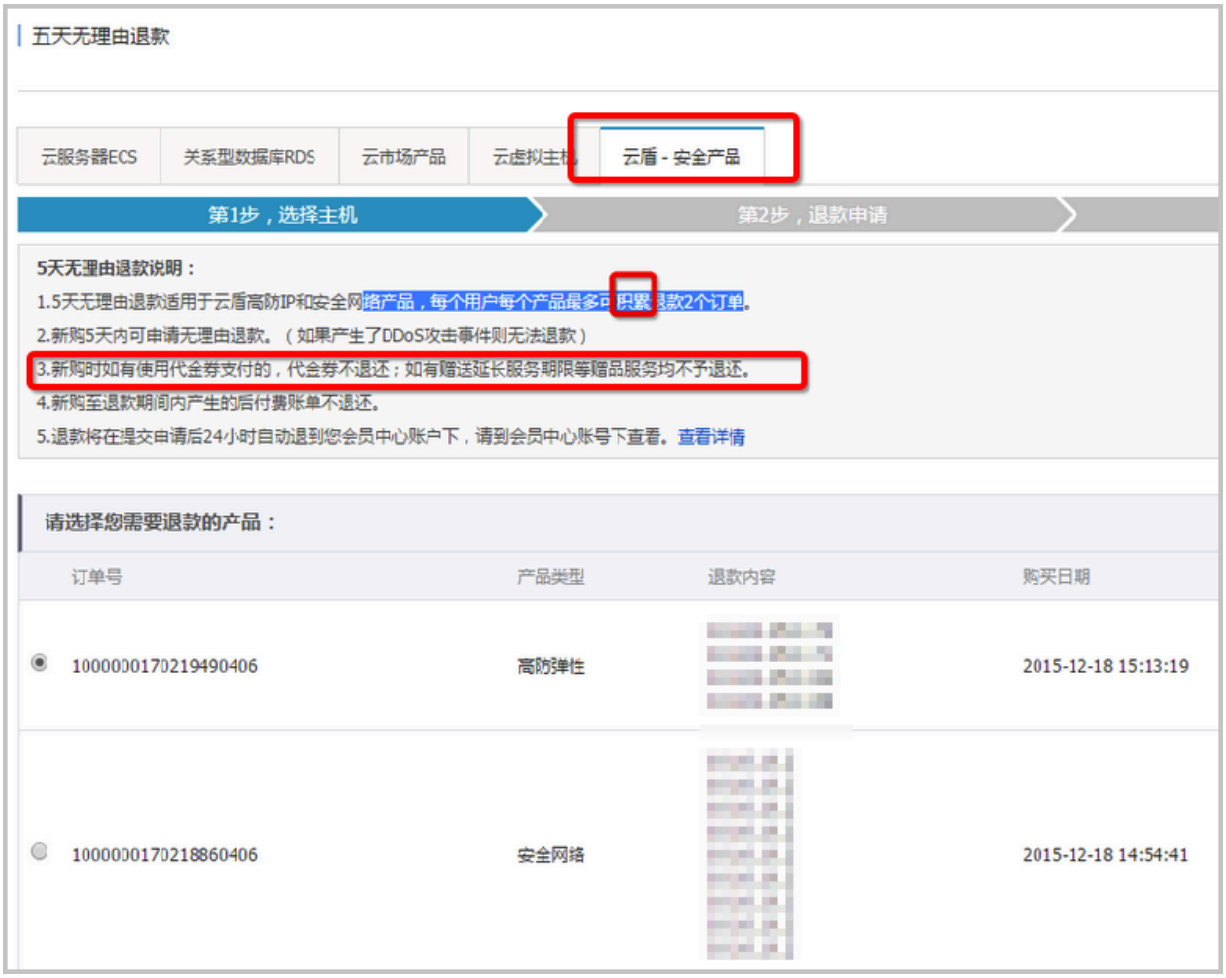
2.6 高防IP退款

云盾 DDoS 高防 IP 支持五天无理由自助退款功能。

说明:

- 对于已使用超过五天的用户，无法进行退款。
- 使用五天无理由退款之前，需要已在高防实例列表页面启用高防 IP，否则无法正常退款。

五天无理由退款详细说明如下:



2.7 升级高防IP实例规格

您购买高防IP实例后，如果所购买的高防IP实例的规格（如线路、保底防护带宽、防护域名数、端口数或业务带宽等）已无法满足您的实际业务需要，您可以随时在云盾DDoS防护管理控制台升级当前高防IP实例规格。

升级高防IP实例规格支持扩展保底防护带宽、防护域名数、端口数和业务带宽。同时，您还可以通过升级高防IP实例对部分线路进行变更。

说明:

不支持降低已购买高防IP实例的保底防护带宽。

目前，升级高防IP实例仅支持以下线路变更方式：

- **电信+联通线路变更为电信+联通+移动线路**
- **BGP线路变更为电信+联通+BGP线路**

说明:

暂时不支持其它线路变更方式。

升级差价计费说明

升级当前高防IP实例规格，您需要补齐升级差价。支付完成后，高防IP实例规格升级即时生效。

保底防护带宽扩展或线路变更

上调保底防护带宽或变更线路所产生的差价部分按以下方式计算：

升级差价金额 =（升级后规格的服务包月价格/30/24）* 剩余时长（小时数）-（当前服务包月价格/30/24）* 剩余时长（小时数）

防护域名数、端口数、业务带宽扩展

增加防护域名数、端口数、业务带宽所产生的差价部分按以下方式计算：

- 防护域名数：新增防护域名按 300 元/月的单价与当前服务剩余时长计算差价。

  说明：
  该高防IP实例所包含的防护域名数超过95个后，每个新增防护域名按 225 元/月的单价计算差价。

- 端口数：新增端口按 50 元/月的单价与当前服务剩余时长计算差价。
- 业务带宽： 新增业务带宽按 100 元／月的单价（每增加 1 M）与当前服务剩余时长计算差价。

  说明：
  该高防IP实例的业务带宽超过 550 M 后，每增加 1 M 按 75 元/月的单价计算差价。

操作步骤

您可以参考以下操作步骤，升级已购买的高防IP实例的规格：

1. 登录云盾DDoS高防IP管理控制台。
2. 定位到资产 > 实例列表，选择高防实例，单击升级

3. 在配置变更页面，扩展保底防护带宽、防护域名数、端口数、业务带宽或变更线路。

4. 完成支付，升级后的高防IP实例规格配置即时生效。

2.8 降配高防IP实例规格

您购买高防IP实例后，如果所购买的高防IP实例的规格（如防护域名数、端口数或业务带宽等）因无法满足您的实际业务而进行过配置升级，但是业务高峰期结束后，您希望重新调整实例规格配置以节省支出，您可以选择降配该高防IP实例。

高防IP实例规格降配支持减少实例的防护域名数、端口数和业务带宽。

降配当前高防IP实例规格时，如果存在差价，差价将自动退还。同时，高防IP实例规格降配即时生效。

减少防护域名数、端口数、业务带宽所产生的差价部分按以下方式计算：

- 防护域名数：减少防护域名按 300 元/月的单价计算。

  说明:
  高防IP实例所包含的防护域名数超过95个时，每个防护域名按 225 元/月的单价计算。

- 端口数：减少端口按 50 元/月的单价计算。
- 业务带宽：降低业务带宽按 100 元／月（每降低 1M）的单价计算。

  说明:
  高防IP实例的业务带宽超过 550 M 时，每减少 1M 按 75 元/月的单价计算。

降配差价金额 = 降配后的实例配置的对应价格（降配后的实例配置的月单价/30/24 * 实例的剩余时长） - 当前实例的现金退款金额（即该实例新购或续费时支付的现金部分的退款金额）

说明:

- 实例的剩余时长按小时计算。
- 当前实例的现金退款金额不含以代金券支付的部分

操作步骤

您可以参考以下操作步骤，降配已购买的高防IP实例的规格：

1. 登录云盾DDoS高防IP管理控制台。
2. 定位到资产 > 实例列表，选择高防IP实例，单击降配。

3. 在配置变更页面，调整防护域名数、端口数和业务带宽降低高防IP实例的配置。

说明:

- 端口和防护域名数不能低于默认的50个。
- 端口和域名数量不能低于当前已经配置使用的数量。

4. 完成支付后，降配后的高防IP实例规格配置即时生效，降配所产生的差价将自动退还至您的阿里云账户。

2.9 防护能力增长规格说明

您可以增加DDoS高防IP的业务带宽，来提高HTTP的正常QPS和HTTPS的正常QPS规格。

默认情况下，单个DDoS高防IP实例包含以下规格限制：

- 业务带宽限制为100M（非DDoS攻击状态下的正常业务消耗带宽）
- HTTP/HTTPS的正常QPS限制为3000（非CC攻击状态下的正常业务请求消耗）

关于DDoS高防IP实例的规格限制的详细说明，请查看*DDoS高防IP产品定价*页面中的其它规格限制说明。

如您需要提高DDoS高防IP实例的规格，请参考下表中的规格增长说明升级您的DDoS高防IP实例的业务带宽。

您每增加指定幅度的业务带宽，即可提升相应的QPS处理能力。

说明：

由于HTTPS耗费更多性能，相比之下提升幅度较小。

增加业务带宽（Mbps）	提升对应的QPS（HTTP）	提升对应QPS（HTTPS）
50	1500	300
100	3000	600
150	4500	900
200	6000	1200
500	15000	3000
1000	30000	6000
2000	60000	12000

3 快速入门

3.1 防护网站业务

3.1.1 概述

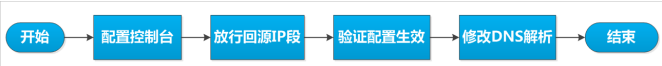
本文档介绍了网站业务用户新购DDoS高防后如何配置上线、切换业务接入高防、并验证防护生效。

读者对象

本文档作为快速入门参考，适用于有以下需求的读者对象：

- 了解网站业务如何使用DDoS高防IP。
- 已购买DDoS高防IP，但不知道如何配置网站业务接入。
- 需要测试、验证、修改、或删除DDoS高防配置。
- 不知道如何配置DNS解析、CNAME地址解析、及A记录解析。

快速入门流程图



一般网站业务接入流程请参考以下步骤：

> 说明：
> 购买高防实例后，您需要先启用高防实例，才可将业务接入DDoS高防IP。

1. *HTTP*网站接入 / *HTTPS*网站接入（根据您实际网站业务选择，进行接入配置）。
2. 源站确认放行*DDoS*高防回源*IP*段。
3. 本地验证配置生效。
4. 修改*DNS*解析，把网站业务切换至DDoS高防IP。

3.1.2 启用高防实例

购买高防实例后，您需要启用该实例才可将您的网站业务或非网站业务接入高防进行防护。您可以参考以下操作步骤，启用您已购买的高防实例。

操作步骤

1. 登录云盾*DDoS*防护管理控制台。
2. 定位到高防IP > 实例列表，选择地域，找到您想要启用的高防实例。

3. 单击立刻启用。
4. 选择线路，单击立即启用。

预期结果

高防实例启用后，您可以根据您的实际情况将您的网站或非网站业务接入该高防实例进行防护。

3.1.3 步骤1：HTTP网站接入

参照以下步骤在DDoS高防IP中接入HTTP协议网站。

操作步骤

1. 登录云盾DDoS防护管理控制台，定位到接入 > 网站，单击添加域名。

2. 在填写域名信息配置界面，填写需要防护的网站信息。

- 在防护网站输入框内填写需要配置防护的网站域名。
- 对于只包含HTTP协议的网站在协议类型选项仅勾选http。
- 源站IP/域名支持两种方式回源。第一种是直接填写真实服务器的IP地址，第二种是填写回源域名（即通过回源域名的DNS解析出真实服务器的IP，再进行流量转发）。

> **说明:**
>
> - `www.abc.com` 和 `abc.com` 需要作为两个不同的域名分别进行配置，否则访问可能出现异常（例如，只配置了 `abc.com`，在访问 `www.abc.com` 时有可能提示无法访问）。
> - 支持泛域名配置，如配置一条`*.a.com`即可同时匹配`1.a.com`、`2.a.com`、`www.a.com`等域名。泛域名仅用占一条配置名额。
> - 如果一个域名对应多个源站IP，可以都填写到源站IP中（最多支持20个IP）。多个源站之间会以IP Hash方式进行轮询实现负载均衡。
> - 源站端口无需配置，根据协议类型自动生成。
> - 网站防护设置只支持80和443端口，其他非标准端口网站业务需要通过非网站的协议转发配置。

3. 单击下一步，进入选择实例和线路配置界面。查看当前已有的高防实例及实例所对应的高防IP，根据实际业务需要选择您的高防IP。

如图所示，可将需要防护网站的域名转发规则绑定到电信、联通、BGP三条线路。

4. 单击确定，完成DDoS高防IP转发规则配置部分。

3.1.4 （可选）步骤1：HTTPS网站接入

参照以下步骤在DDoS高防IP中接入HTTPS协议网站。

操作步骤

1. HTTPS网站接入配置，与*HTTP网站接入*的配置步骤基本相同。只需要在填写域名信息时，在协议类型选项同时勾选http和https。

   说明:

   网站只有HTTPS业务（没有HTTP业务）的情况，也需要勾选http协议类型。

   勾选https协议类型后，您会看到提示信息："域名添加完成之后，请继续添加证书和私钥"。

2. 单击下一步，选择实例和线路。单击确定，完成域名转发规则的配置。

3. 在域名列表中，您可以查看刚添加的域名的配置情况，业务状态栏中也会提示您需要上传证书。

4. 复制证书和私钥文本内容，完成证书上传。

   一般如pem、cer、crt等证书格式，可用文本编辑器直接打开进行复制。其它特殊格式（如PFX、P7B等）的证书需要先转换成pem格式。

   详情参考*高防HTTPS证书转换成pem格式的方法汇总*。

   说明:

   如果有多个证书文件（如证书链），可拼接合并后一起上传。

   可识别的证书样例格式如下：

   ```
   -----BEGIN CERTIFICATE-----
   62EcYPWd2Oy1vs6MTXcJSfN9Z7rZ9fmxWr2BFN2XbahgnsSXM48ixZJ4krc+1M+
   j2kcubVpsE2
   cgHdj4v8H6jUz9Ji4mr7vMNS6dXv8PUkl/qoDeNGCNdyTS5NIL5ir+g92cL8IGOk
   jgvhlqt9vc
   65Cgb4mL+n5+DV9uOyTZTW/MojmlgfUekC2xiXa54nxJf17Y1TADGSbyJbsC0Q9
   nIrHsPl8YKk
   vRWvIAqYxXZ7wRwWWmv4TMxFhWRiNY7yZIo2ZUhl02SIDNggIEeg==
   -----END CERTIFICATE-----
   ```

   私钥样例格式如下：

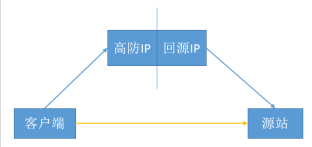
   ```
   -----BEGIN RSA PRIVATE KEY-----
   ```

```
DADTPZoOHd9WtZ3UKHJTRgNQmioPQn2bqdKHop+B/dn/4VZL7Jt8zSDGM9sTMThL
yvsmLQKBgQ
Cr+ujntC1kN6pGBj2Fw2l/EA/W3rYEce2tyhjgmG7rZ+A/jVE9fld5sQra6ZdwBcQJ
aiygoIYo
aMF2EjRwc0qwHaluq0C15f6ujSoHh2e+D5zdmkTg/3NKNjqNv6xA2gYpinVDz
FdZ9Zujxvuh9o
4Vqf0YF8bv5UK5G04RtKadOw==
-----END RSA PRIVATE KEY-----
```

5. 单击确定。证书上传完毕后，HTTPS业务状态显示为正常。

3.1.5 步骤2：放行回源IP段

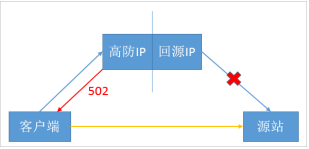
DDoS高防作为一个反向代理，其中包含了一个Full NAT的架构。



没有启用DDoS高防代理时，对于源站来说真实客户端的地址是非常分散的，且正常情况下每个源IP的请求量都不大。

启用DDoS高防代理后，由于高防回源的IP段固定且有限，对于源站来说所有的请求都是来自高防回源IP段，因此分摊到每个回源IP上的请求量会增大很多（可能被误认为回源IP在对源站进行攻击）。此时，如果源站有其它防御DDoS的安全策略，很可能对回源IP进行拦截或者限速。

例如，最常见的502错误，即表示高防IP转发请求到源站，但源站却没有响应（因为回源IP可能被源站的防火墙拦截）。



所以，在配置完转发规则后，强烈建议关闭源站上的防火墙和其他任何安全类的软件（如安全狗等），确保高防的回源IP不受源站本身安全策略的影响。同时，建议您参考高防源站保护通过安全组或白名单功能为您的源站配置保护措施。

DDoS高防回源IP段

您可在云盾DDoS防护管理控制台中，单击高防回源IP段，查看详细的高防IP回源地址段。

3.1.6 步骤3：验证配置生效

在云盾DDoS防护管理控制台配置完成后，DDoS高防预期可以把请求高防IP的报文转发到源站（真实服务器）。为了最大程度保证业务的稳定，我们建议在切换DNS解析之前先进行本地的测试。

操作步骤

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

   a) 找到Hosts文件。一般Hosts文件在 C:\Windows\System32\drivers\etc\ 文件夹中。

   b) 用记事本或Notepad++等文本编辑器，打开hosts文件。

   c) 在最后一行添加如下内容：`高防IP地址 网站域名`。

   以“www.aliyundemo.com”为例，在hosts文件最后一行添加如下内容：

   > 说明：
   > 前面的高防IP地址为添加域名转发规则时所选择的高防IP地址。
   >
   > 如果配置时，选择了多个线路的高防IP（如电信、联通、BGP三条线路），可以分别绑定三个IP，分三次进行测试。

   d) 修改hosts文件后保存。

2. 在本地计算机对被防护的域名运行Ping命令。
   预期解析到的IP地址是在hosts文件中绑定的高防IP地址。如果依然是源站地址，可尝试刷新本地的DNS缓存（在Windows的命令提示符中运行ipconfig/flushdns命令。）

3. 确认hosts绑定已经生效（域名在本地解析为高防IP）后，打开浏览器，输入域名访问被防护网站。
   如果高防IP服务的配置正确，网站预期能正常访问。

   如果网站无法正常访问，请确认步骤1、步骤2中的配置是否正确。如问题依然存在，请联系阿里云售后支持。

3.1.7 步骤4：修改DNS解析

最后，修改DNS解析，使所有用户的访问都先经过DDoS高防再回到源站（相当于将所有流量长牵引到高防IP）。

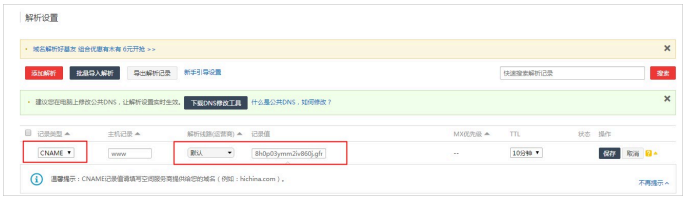
各个DNS解析提供商的配置原理相同，具体配置步骤可能有细微差别，本文以万网配置为例。

1. 登录万网域名控制台，进入域名解析设置。

以图中的域名aliyundemo.com为例，当前的域名解析采用A记录的方式，默认线路（除联通以外的线路，包含电信、移动、教育网、铁通、海外等线路）的@和www记录（即用户直接访问域名“aliyundemo.com”或者“www.aliyundemo.com”）都是解析到源站IP地址为11.11.11.11的服务器，而联通线路则是解析到源站IP地址为22.22.22.22的服务器。

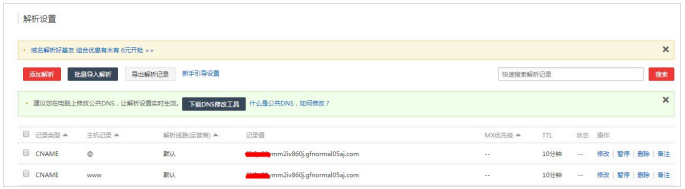
2. 接入DDoS高防后，需要修改域名解析配置让域名解析到高防IP上。

   目前，支持CNAME解析和A记录解析两种方式，推荐使用*CNAME*方式接入。



把记录类型改为CNAME，在记录值内输入CNAME地址。

在配置域名转发规则时，云盾DDoS防护管理控制台已自动生成该域名的CNAME地址，并且提供分线路智能解析功能。因此，CNAME解析只需要配置默认线路的解析即可。



说明:

如果您的域名解析不支持或者无法配置CNAME解析（例如，已配置MX记录的域名会提示@主机记录和MX记录冲突），可以使用A记录进行域名解析。配置方法与普通A记录配置方法相同。

推荐按照以下方式进行A记录解析配置：

三线套餐用户：

- 设置电信线路A记录解析到电信的高防IP。
- 设置联通线路A记录解析到联通的高防IP。
- 设置默认线路A记录解析到BGP的高防IP。

二线套餐用户：

- 设置默认线路A记录解析到电信的高防IP。
- 设置联通线路A记录解析到联通的高防IP。

在配置域名解析完后，可通过一些在线测试工具（如17ce等）测试域名的解析情况。

DNS的完全生效时间，根据各地DNS解析的收敛时间不同而不同。

> 说明:
> 请务必确保把所有业务都切换到DDoS高防，不然恶意攻击者还是能够通过未解析到DDoS高防的业务找到源站服务器IP地址，从而绕过DDoS高防直接攻击源站。

如果源站暴露，请参考使用高防后源站IP暴露的解决办法。

3.2 防护非网站业务

3.2.1 概述

本文档介绍了非网站业务（如端游、手游、APP等）用户新购DDoS高防后如配置上线，切换业务接入高防，并验证防护生效。

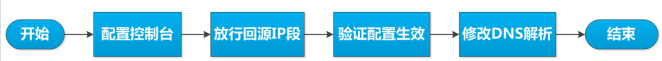
> 说明:
> 与网站业务不同，非网站业务配置后只进行四层转发。DDoS高防不会解析七层报文的内容，也不提供基于七层报文的防护（如CC攻击、Web攻击等），只支持四层防护（如SYN Flood、UDP Flood等）。

读者对象

本文档作为快速入门参考，适用于有以下需求的读者对象：

- 了解非网站业务如何使用高防IP。
- 已购买DDoS高防IP，但不知道如何配置业务接入。
- 需要测试、验证、修改、或删除DDoS高防配置。
- 不知道如何配置DNS解析、CNAME地址解析、及A记录解析。

快速入门流程图



一般非网站类业务接入流程请参考以下步骤：

> 说明:
> 购买高防实例后，您需要先启用高防实例，才可将业务接入DDoS高防IP。

1. 控制台配置四层转发配置。
2. 源站上确认放行高防回源IP段。
3. 本地验证配置生效。
4. 修改DNS解析，把全部业务切换至DDoS高防IP。

3.2.2 步骤1：配置四层转发

非网站业务只支持四层转发，不支持七层防护（如WAF和CC防护），也不支持黑白名单。

操作步骤

1. 登录云盾DDoS防护管理控制台，定位到接入 > 非网站。

   在非网站页面，可选择高防实例和高防IP。

2. 选择需要配置规则的高防IP后，单击添加规则。
3. 选择转发协议（目前支持TCP和UDP），设置转发端口（需要通过高防IP的哪个端口来访问，一般情况选择跟源站相同端口）。然后，填写源站端口（源站提供业务服务的真实端口）和源站IP。

> 说明：
>
> - 如果一个端口对应多个源站IP，可以都填写到源站IP中（最多支持20个IP）。多个源站之间会以轮询方式实现负载均衡；
> - 非网站转发端口不支持80端口和UDP的53端口，网站类业务请直接在网站业务接入中配置。

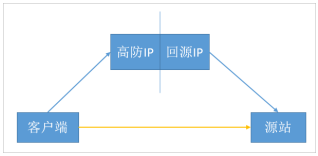
4. 单击确定。

3.2.3 步骤2：放行回源IP段

本文目的是为了避免源站将DDoS高防的回源IP拦截而影响业务，而不是源站保护（只允许经过DDoS高防的请求访问源站）。

如果您想要配置源站保护，请参考高防源站保护。

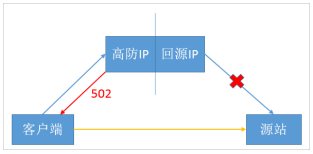
DDoS高防作为一个反向代理，其中包含了一个Full NAT的架构。



没有启用DDoS高防代理时，对于源站来说真实客户端的地址是非常分散的，且正常情况下每个源IP的请求量都不大。

启用DDoS高防代理后，由于高防回源的IP段固定且有限，对于源站来说所有的请求都是来自高防回源IP段，因此分摊到每个回源IP上的请求量会增大很多（可能被误认为回源IP在对源站进行攻击）。此时，如果源站有其它防御DDoS的安全策略，很可能对回源IP进行拦截或者限速。

例如，最常见的502错误，即表示高防IP转发请求到源站，但源站却没有响应（因为回源IP可能被源站的防火墙拦截）。



所以，在配置完转发规则后，我们强烈建议关闭源站上的防火墙和其他任何安全类的软件（如安全狗等），确保高防的回源IP不受源站安全策略的影响。

DDoS高防回源IP段

您可登录云盾DDoS防护管理控制台，定位到实例列表，单击高防回源IP段，查看详细的高防IP回源地址段。

3.2.4 步骤3：验证配置生效

在云盾DDoS防护管理控制台配置完成后，DDoS高防预期可以把请求高防IP对应端口的报文转发到源站（真实服务器）的对应端口。为了最大程度保证业务的稳定，我们建议在全面切换业务之前先进行本地的测试。

直接用IP访问（不需要域名）的业务

有的四层业务（如游戏业务）可能不需要域名，是直接通过IP来进行交互的。

例如，高防IP是99.99.99.99，配置了端口1234的转发，源站IP是11.11.11.11，对应服务端口也是1234。在完成前两步的配置后，可以直接本地通过telnet命令访问高防IP 99.99.99.99的1234端口，telnet命令能连通则说明转发成功。

或者，如果能在本地客户端直接填写服务器IP，也可以直接填入高防IP进行测试。

需要用域名访问的四层业务

对于需要通过域名来访问的业务（如客户端中使用的服务器地址是域名而不是IP），可通过以下两种方法来验证配置是否生效：

- 修改本地hosts文件
  1. 首先修改本地*hosts*文件，使本地对于被防护站点的请求经过高防。

     以Windows操作系统为例：

     a. 找到Hosts文件。一般Hosts文件在 `C:\Windows\System32\drivers\etc\` 文件夹中。
     b. 用记事本或Notepad++等文本编辑器，打开hosts文件。
     c. 在最后一行添加如下内容：`高防IP地址 网站域名`。以“www.aliyundemo.com”为例，在hosts文件最后一行添加如下内容：

     d. 修改hosts文件后保存。
  2. 在本地计算机对被防护的域名运行Ping命令。

     预期解析到的IP地址是在hosts文件中绑定的高防IP地址。如果依然是源站地址，可尝试刷新本地的DNS缓存（在Windows的命令提示符中运行ipconfig/flushdns命令。）
  3. 确认本地解析已经切换到高防IP以后，使用原来的域名进行测试，如果能正常访问则说明配置已经生效。
- 直接通过CNAME地址访问服务器

如果客户端支持填写服务器域名，可以把原来的域名替换成DDoS高防服务已分配的接入CNAME地址，测试访问是否正常。

如果无法正常访问，请确认步骤1、步骤2中的配置是否正确。如问题依然存在，请联系阿里云售后支持。

3.2.5 （可选）步骤4：修改DNS解析

本步骤仅针对使用四层业务、同时还需要使用域名来指定服务器地址的业务。例如，某游戏客户端，需要填写域名“aliyundemo.com”作为服务器地址，或是这个域名已经写在客户端程序中。

> 说明:
> 如果通过直接指定IP进行访问的四层业务，则无需进行以下步骤配置。

修改DNS解析，使所有用户的访问都先经过DDoS高防再回到源站（相当于将所有流量长牵引到高防IP）。

各个DNS解析提供商的配置原理相同，具体配置步骤可能有细微差别，本文以万网配置为例。

1. 登录万网域名控制台，进入域名解析设置。

以图中的域名aliyundemo.com为例，当前的域名解析采用A记录的方式，默认线路（除联通以外的线路，包含电信、移动、教育网、铁通、海外等线路）的@和www记录（即用户直接访问域名“aliyundemo.com”或者“www.aliyundemo.com”）都是解析到源站IP地址为11.11.11.11的服务器，而联通线路则是解析到源站IP地址为22.22.22.22的服务器。

2. 接入DDoS高防后，需要修改域名解析配置让域名解析到高防IP上。

推荐按照以下方式进行A记录解析配置：

- 三线套餐用户：
  - 设置电信线路A记录解析到电信的高防IP。
  - 设置联通线路A记录解析到联通的高防IP。
  - 设置默认线路A记录解析到BGP的高防IP。
- 二线套餐用户：

- 设置默认线路A记录解析到电信的高防IP。
- 设置联通线路A记录解析到联通的高防IP。

在配置域名解析完后，可通过一些在线测试工具（如17ce等）测试域名的解析情况。

DNS的完全生效时间，根据各地DNS解析的收敛时间不同而不同。

说明:

请务必确保把所有业务都切换到DDoS高防，不然恶意攻击者还是能够通过未解析到DDoS高防的业务找到源站服务器IP地址，从而绕过DDoS高防直接攻击源站。

如果源站暴露，请参考使用高防后源站IP暴露的解决办法。

4 用户指南

4.1 业务接入配置

4.1.1 网站业务CNAME方式接入配置

DDoS高防IP目前支持CNAME接入和A记录接入两种方式，推荐方式为CNAME接入。

CNAME是DNS的别名记录，可以理解为一个跳转。例如，域名www.abc.com, 对应的真实源站IP为1.1.1.1，对应的CNAME为abcde12345.alicloudddos.com。

那么，使用A记录时，DNS将www.abc.com A记录解析到 1.1.1.1；使用CNAME记录时，DNS将www.abc.com CNAME记录到 abcde12345.alicloudddos.com。

后者对应的真实IP是您不需要关心也不需要配置的，客户端会自动查询这个CNAME记录，最终得到一个IP（1.1.1.1）。

在接入DDoS高防IP的过程中，假设高防IP为2.2.2.2（电信线路）,3.3.3.3（联通线路）,4.4.4.4（BGP线路），则对于同一个域名，在三条线路中生成的CNAME记录都是一样的 。您只需要配置一条CNAME解析，即把www.abc.com 解析到这个CNAME记录，这个CNAME记录对应哪些IP，交给阿里云完成即可。

重点是，一个CNAME记录对应的实际IP可以有多个，也是可以改变的，且这个过程对您来说都是透明无感知的。然而，如果使用A记录，一旦需要更换解析的IP，则必须手动更改解析配置。

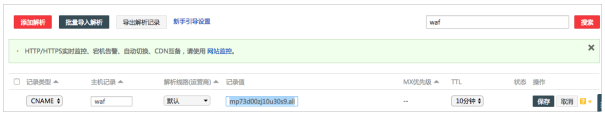
CNAME接入有什么好处?

- CNAME接入模式更加方便，您只需要在域名解析服务商处（如万网云解析或者DNSPod）修改一次解析配置即可生效，实现零部署、零运维。
- 当某条线路的高防IP出现异常时，使用CNAME解析的域名可以被自动切换到其他的高防IP（如华北联通线路故障或拥塞，可自动调度到东北联通去）。
- 如果您使用的是三线套餐，当某条线路被攻击导致黑洞时，CNAME可以自动调度解析到其他可用的线路上去，避免原本解析到该线路的部分业务受到影响，保证业务的可用性。

网站接入高防CNAME的步骤

1. 购买高防IP。
2. 登录云盾DDoS防护管理控制台，添加域名，配置转发规则。

3. 至域名服务商处修改DNS解析配置，将域名解析至高防的CNAME记录。



4. 等待DNS生效（大约在几分钟内），网站即完成了通过CNAME接入DDoS高防。
5. 测试网站访问是否正常。

DDoS高防CNAME解析的时候对于运营商线路如何解析？

一般针对电信线路会解析到电信高防，联通线路解析到联通高防，其他运营商（如教育网、移动、铁通、长城宽带等）解析到BGP高防。

已配置分链路解析，使用CNAME接入后如何配置？

一般情况下您只需要一条默认线路的CNAME解析即可替换之前的分链路解析，智能解析的过程由阿里云自动完成。

DDoS高防提供的CNAME地址已经具备分链路解析的能力，我们会检测该CNAME记录对应的域名在电信、联通、BGP的配置是否存在，如果存在就会在这三条线路中自动进行分链路解析。

相关链接

- *CNAME*自动调度功能说明
- *CNAME*接入状态说明

4.1.2 非网站业务CNAME方式接入配置

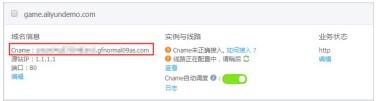
本文通过一个实例说明如何使用CNAME解析的方式将您的四层业务接入高防。

大多数情况下，四层业务接入（非网站防护）场景下客户端直接指定访问高防的IP即可。但在某些场景下，您可能需要用域名来接入您的四层业务，这种情况下，您可以通过添加一个七层的域名来实现用一个相同的CNAME智能解析到不同线路的高防IP，并实现CNAME自动切换的功能。

假设，您希望用户通过解析游戏服务器的域名（game.aliyundemo.com）来获取服务器对应的IP（也就是高防IP），同时游戏的TCP端口为1234和5678，源站为1.1.1.1，则可以参考以下步骤进行配置：

步骤1：配置网站转发规则（获取CNAME）

首先，在网站防护中添加一条game.aliyundemo.com的转发规则（同时绑定电信、联通、BGP三条线路）。这样，不同线路的高防IP都会使用相同的CNAME，步骤3中的DNS解析将使用这个CNAME。



> **说明:**
> 这里的源站IP和协议可随意填写，因为这条规则对应的并不是实际业务需要的1234或5678端口。对这两个端口的访问请求会按照步骤2中的非网站业务转发规则经过高防IP。

当然，如果这个域名还有真实的网站业务，则必须填写正确地协议类型和源站IP。同时，四层业务防护的解析依然可以使用这个CNAME。

步骤2： 配置非网站转发规则

此处的配置方式不变，按照非网站接入的配置方法配置转发规则即可。

两条转发规则配置如下：

> **说明:**
> 步骤1中启用的高防IP都要配置相应的非网站转发规则，支持规则的导入导出。

步骤3： 修改DNS解析到七层域名

在DNS解析处，将game.aliyundemo.com这个域名配置CNAME解析到步骤1中网站防护生成的CNAME。

至此，您的客户端就可以通过域名分线路智能解析高防IP，而高防IP服务也可以基于四层转发的配置来正确转发请求到源站了。

另外，如果您需要对四层业务配置*CNAME*自动调度，也可在这个域名下开启。在使用CNAME解析后，将提供与网站防护相同的调度效果。

4.1.3 CNAME接入状态说明

对于接入高防IP服务的网站类用户，建议您采用CNAME接入的方式。

具体请参考*CNAME*接入的方式。

CNAME接入有以下优点：

- CNAME接入模式更加方便。您只需要在域名解析服务商处（如阿里云解析或者dnspod）修改一次解析配置即可生效，实现零部署、零运维。

- 当某条线路的高防IP出现异常时，使用CNAME解析的域名将自动切换到其他的高防IP。例如，华北联通线路故障或拥塞，可自动调度到东北联通。
- 如果您使用三线套餐，当BGP线路（基础防护带宽上限20G，弹性防护带宽上限100G）被攻击导致黑洞时，CNAME可以自动调度解析到电信和联通线路上去，避免原本解析到BGP线路的部分业务受到影响。

在高防IP管理控制台的网站防护配置中，可以查看当前配置域名是否使用CNAME接入。判定依据为：

- 如果当前域名已经配置了CNAME解析到高防IP，则提示已接入高防防护。

- 如果当前域名没有配置CNAME解析（例如使用A记录解析方式，或者CNAME解析配置不正确），则会提示CNAME未正确接入。

说明：

有此提示并不代表解析或者业务一定有异常。例如，无法使用CNAME解析的域名，通过A记录解析方式的域名也可以正常使用。如解析后您的业务访问正常，可忽略此提示。

4.1.4 CNAME自动调度

高防IP服务默认提供CNAME自动调度功能，无需额外开启。

当某个线路的高防IP进入黑洞时，高防IP服务会自动根据所设置的流量调度方式将业务流量切换到其他正常的线路，提供灾备能力，保证业务的连续性和可用性。因此，建议您通过修改域名DNS解析CNAME记录的方式将业务流量牵引到到高防IP实例。

说明：

如果您通过修改域名DNS解析A记录的方式牵引业务流量到高防IP实例，则无法基于CNAME自动调度功能实现流量调度管理且不具备冗余灾备能力，建议您使用CNAME方式接入高防IP服务或者选用具备自动灾备能力的新BGP高防IP服务。

基于CNAME自动调度功能，目前高防IP服务提供负载均衡方式和优先级两种流量调度方式。

当您采用负载均衡的流量调度方式时，如果您的高防IP实例包含电信、联通、BGP三个线路的高防IP，将根据以下原则进行流量调度：

- 当BGP线路的高防IP进入黑洞时，网站域名将自动解析到电信线路（实际解析切换的生效时间根据DNS的缓存生效时间而定）。
- 当BGP线路和联通线路的高防IP都进入黑洞时，则原本解析到联通和BGP线路网站域名访问请求都会解析到电信线路的高防IP（实际解析切换的生效时间根据DNS的缓存生效时间而定）。
- 如果该高防IP实例所拥有的所有线路全部进入黑洞时，则无法再进行域名解析的自动调度。

说明：

CNAME自动切换一般可一分钟内完成并生效，即在一分钟内该网站域名CNAME在DNS服务器中解析得到的IP切换成正常线路的IP。但是，由于客户端实际生效时间依赖于本地DNS缓存和更新时间，可能存在一定延迟。

优先级方式

当您采用优先级的流量调度方式时，高防IP服务将根据您所设置的线路优先级进行流量调度，业务流量将优先调度至当前可用的优先级最高的高防IP线路。

基于CNAME自动调度功能的具体流量调度方式配置方法，请查看流量调度方式管理。

4.1.5 修改业务源站IP

在使用高防IP配置了非网站防护或网站防护后，您可以根据需要来修改源站IP。

参照以下步骤，来修改非网站接入的源站IP。

1. 登录云盾DDoS防护管理控制台，并前往接入 > 非网站页面。
2. 选择实例，并选择高防IP。
3. 选择规则，并单击其操作列下的编辑。
4. 修改源站IP后，单击操作列下的确定。

说明：

如果非网站接入有多条线路，则每条线路的转发配置都需要修改。

网站接入

参照以下步骤，来修改网站接入的源站IP。

1. 登录云盾DDoS防护管理控制台，并前往接入 > 网站页面。
2. 选择需要修改源站IP的网站实例，单击其域名信息下的回源编辑。

3. 在回源编辑页面，单击编辑源站。
4. 修改源站IP后，单击确定。

说明:
源站 IP 修改后，网站需要一定时间来下发配置。因此，在配置下发完成前，访问请求还会转发到之前的源站 IP。

4.1.6 修改网站业务高防线路和源站配置

通常来说，每个高防IP实例至少拥有一条高防IP线路，同时您的账号下还可能拥有多个高防IP实例，因此大多数情况下您的账号都会拥有多条高防IP线路。

在将网站域名添加至高防IP实例进行防护时，您已经为该域名配置至少一条高防IP线路作为转发线路，同时为该转发线路指定源站地址。

在实际使用过程中，您可能需要灵活调整该网站域名的高防IP实例的转发线路或者源站配置来满足实际业务需要。

例如，通过修改某网站域名的高防IP转发线路和源站配置，您可以满足类似以下业务需求：

- 在原有电信和联通高防IP线路的基础上增加移动线路或增加其它高防IP实例的电信线路。
- 默认将来自移动网内的访问请求通过移动高防IP线路进行转发，而不需要跨网访问其它高防IP线路。
- 将来自电信网内的访问请求通过多个电信高防IP线路进行转发，实现业务访问流量平均分配至多个电信高防IP线路进行转发。

前提条件

确认需要修改的网站域名已经配置接入高防IP实例进行防护。

说明:
如果您还未将需要配置的网站域名接入高防IP实例，请参考*HTTP网站接入*或*HTTPS网站接入*将您的域名添加至已购买的高防IP实例。

参考以下步骤，修改指定网站域名的高防IP转发线路和源站配置。

说明:
建议您先使用测试域名熟悉操作步骤后，再进行实际业务的配置修改。同时，建议您在业务低峰期修改网站域名的高防IP转发线路和源站配置，避免对实际业务产生影响。

1. 登录*云盾DDoS防护管理控制台*，定位到接入 > 网站页面。
2. 定位到需要修改配置的网站域名记录，单击域名信息区域中的回源编辑，打开回源编辑页面。

说明:

您也可以单击该网站域名记录的实例与线路区域中的编辑，打开回源编辑页面。

3. 根据您的业务需要，修改该网站域名的高防IP转发线路和源站配置。

   · 添加转发线路

   a. 单击添加转发线路，增加该网站域名的转发线路。

      例如，在原有的电信和联通转发线路的基础上，增加其他高防IP线路。

   b. 在添加转发线路对话框中，选择回源模式，填写源站信息，单击下一步。

   c. 选择需要增加的高防IP实例和线路，单击启用。

说明:

您可以选择启用多个高防IP实例的多个线路。

说明:

在添加转发线路对话框中，该网站域名已配置的高防IP线路类型的所有线路都将显示为灰色并标识为已占用。例如，该网站域名已经配置电信和联通的转发线路，所有高

防IP实例的电信和联通线路都显示为已占用。您需要通过编辑线路功能修改已经配置的高防IP转发线路，具体操作方法请参考下文编辑线路。

d. 单击确定，在回源编辑页面中即显示已添加的转发线路记录。

· 编辑线路

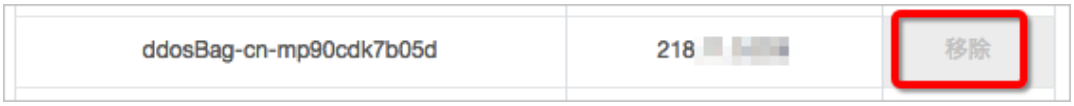
a. 选择已配置的转发线路，单击编辑线路，可修改该转发线路所对应的高防IP线路。

- 添加对应的高防IP实例：在编辑线路对话框中，选择高防IP实例，单击启用。

说明:
您可以为一条转发线路配置多个高防IP实例，实现业务访问流量平均分配至多个高防IP实例进行转发。

- 移除对应的高防IP实例：在编辑线路对话框中，选择高防IP实例，单击移除。

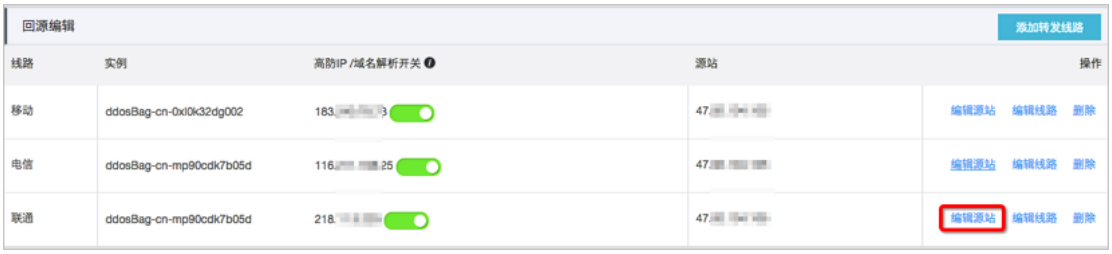
说明:
如果某个高防IP实例对应的移除显示为灰色，表示该转发线路已经启用该高防IP实例且域名解析开关已开启。



如果需要从转发线路中移除该高防IP实例，您需要先在回源编辑页面关闭转发线路中该高防IP实例对应的域名解析开关，然后在编辑线路对话框中移除该高防IP实例。

- 编辑源站

  a. 选择已配置的转发线路，单击编辑源站，可修改该线路的源站配置。



  b. 在编辑源站对话框中，选择回源模式，填写源站信息，单击确定。

> 说明:
> 源站配置变更需要五分钟后才能生效时间，请您耐心等待。

- 删除转发线路

  选择已配置的转发线路，单击删除，删除该线路类型的所有转发线路配置记录。删除线路类型的转发记录后，在添加转发线路对话框中该线路类型的高防IP线路将不再显示为已占用状态，可以直接启用。

> 说明:
> 如果该类型的转发线路是该网站域名所配置的唯一的转发线路，您无法删除该转发线路。

4.1.7 高防线路默认解析说明

介绍了高防线路的默认解析规则。

- 默认情况下，电信线路会解析到电信高防，联通线路解析到联通高防，其他运营商（如教育网、移动、铁通、长城宽带等）解析到BGP高防。
- 当您停止电信或联通线路的时候，默认会将电信或联通用户解析到BGP高防。

- 当您停止BGP线路的时候，默认会将移动、教育网、小运营商等用户解析到电信高防。

4.2 网络七层防护设置

4.2.1 HTTP(S) Flood攻击防护设置

DDoS高防IP服务针对HTTP(S) flood攻击（CC攻击）提供四种防护模式供您选择。

- 正常模式：默认的CC安全防护模式。网站无明显流量异常时建议采用此模式。

  正常模式的CC攻击防护策略相对宽松，可以防御一般的CC攻击，对于正常请求不会造成误杀。
- 攻击紧急模式：当发现网站响应、流量、CPU、内存等指标出现异常时，可切换至此模式。

  攻击紧急模式的CC攻击防护策略相对严格。相比正常模式，此模式可以防护更为复杂和精巧的CC攻击，但可能会对少部分正常请求造成误杀。
- 严格模式：严格模式的CC攻击防护策略较为严格。同时，该模式会对被保护网站的所有访问请求实行全局级别的人机识别验证，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。

  > 说明:
  > 对于严格模式的全局算法认证，如果是真人通过浏览器的访问请求均可以正常响应；但如果被访问网站的业务是API或原生app应用，将无法正常响应该算法认证，导致网站业务无法正常访问。
- 超级严格模式：超级严格模式的CC攻击防护策略非常严格。同时，该模式会对被保护网站的所有访问请求实行全局级别的人机识别验证，即针对每个访问者都将进行验证，只有通过认证后后才允许访问网站。

  相比于严格模式，超级严格模式所使用的全局算法认证在验证算法中还增加反调试、反机器验证等功能。

  > 说明:
  > 对于超级严格模式的全局算法认证，如果是真人通过浏览器的访问请求均可以正常响应（可能存在极少部分浏览器处理异常导致无法访问，关闭浏览器后再次重试即可正常访问）；但如果被访问网站的业务是API或原生app应用，将无法正常响应该算法认证，导致网站业务无法正常访问。

DDoS高防IP服务的CC安全防护功能支持防护模式自动切换，即根据您为被防护网站域名所设定的QPS阈值自动切换CC安全防护模式。

当所防护的网站的QPS值超过您所设定的QPS阈值且持续一段时间后，将自动触发CC安全防护模式的切换，从当前的防护模式自动切换至指定防护模式（例如，严格模式或超级严格模式）；当网站

的QPS值恢复到所设定的QPS阈值以下且持续一段时间后，CC安全防护模式将自动恢复至切换前的防护模式（例如，正常模式）。

> 说明:
> 如果您需要启用CC安全防护模式的自动切换功能，请提交工单申请开通。

操作步骤

默认情况下，您的高防IP实例所防护的网站域名采用正常CC安全防护模式，您可以根据实际情况自由调整防护模式。

1. 登录云盾DDoS防护管理控制台。
2. 定位到防护 > 防护设置 > Web攻击防护页面，选择高防IP实例，选择已接入防护的域名。

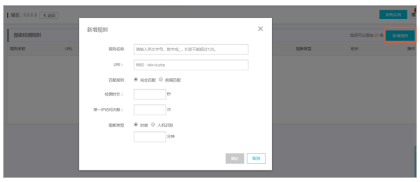
> 说明:
> 您也可以定位到接入 > 网站页面，找到您已接入防护的域名，单击安全防护栏中的防护设置，跳转到Web攻击防护设置页面。

3. 定位到CC安全防护区块，选择CC攻击防护模式。

自定义规则

DDoS高防IP服务的CC安全防护功能还支持通过自定义防护规则进行更精准的HTTP Flood攻击拦截。您可以通过自定义CC攻击防护规则，针对需要重点保护的URL配置防护策略。

您可以在已接入防护的域名的Web攻击防护设置页面，定位到CC安全防护区块，启用自定义规则防护，并单击设置来配置自定义CC防护规则。



CC安全防护设置最佳实践

CC安全防护各模式的防护效果排序依次为：超级严格模式 > 严格模式 > 紧急模式 > 正常模式。同时，各防护模式导致误杀的可能性排序依次为：超级严格模式 > 严格模式 > 紧急模式 > 正常模式。

正常情况下，建议您为已接入防护的域名选择正常CC安全防护模式。该模式的防护策略较为宽松，只会针对访问频次较大的IP进行封禁。当您的网站遭遇大量HTTP Flood攻击时，且正常模式的安全防护效果已经无法满足要求，建议您切换至攻击紧急模式或严格模式。

说明:

- 如果您的网站业务是API或原生APP应用，由于无法正常响应严格、超级严格模式中的相关算法认证，无法使用严格或超级严格模式进行防护。因此，需要通过配置CC安全防护自定义规则对被攻击的URL配置针对性的防护策略拦截攻击请求。
- 如果您网站本身有其他第三方支付回调，或者服务器、端回调，一般无法正常响应严格、超级严格模式中的相关算法认证，需要整理相关回调IP，加入到网站防护设置中的白名单。

4.2.2 黑白名单设置

高防IP服务支持对已接入防护的网站域名设置黑名单和白名单。

背景信息

- 对于已配置白名单的网站域名，来自白名单中的IP或IP段的访问请求将被直接放行，且不经过任何防护策略过滤。
- 对于已配置黑名单的网站域名，来自黑名单中的IP或IP段的访问请求将会被直接阻断。

说明:

黑白名单的配置仅针对单个网站域名生效，而不是针对整个高防IP实例。对于单个网站域名，您最多可分别配置200条黑白名单记录。黑白名单记录支持单个IP或者IP/掩码的格式。

对于访问量较大的恶意IP，您可以将这类IP添加至黑名单进行拦截；对于企业内部办公网的IP段、业务接口调用IP或其它已确认正常的IP，可以将这类IP添加至白名单予以放行，来自白名单中的IP的访问请求和流量将不会被拦截。

操作步骤

1. 登录云盾DDoS防护管理控制台。
2. 定位到防护 > 防护设置 > Web攻击防护页面，选择高防IP实例，选择已接入防护的域名。

说明:

您也可以定位到接入 > 网站页面，找到您已接入防护的域名，单击安全防护栏中的防护设置，跳转到Web攻击防护设置页面。

3. 定位到黑白名单区块，单击设置。

说明:

配置黑白名单必须启用CC安全防护功能。

- 选择黑名单页签，填写需要进行拦截的恶意IP或IP段，单击保存。
- 选择白名单页签，填写需要被放行的IP或IP段，单击保存。

说明:

- IP或IP段支持以IP或IP/掩码的格式填写，支持分别配置最多200条黑白名单记录，多条记录之间用英文“,”进行分隔。
- 黑白名单配置暂不支持非网站防护。
- 黑白名单配置完成后即刻生效。
- 黑白名单配置后，对在该网站域名绑定的所有高防IP实例的防护IP生效。

4.2.3 流量调度方式管理

通常来说，每个高防IP实例至少拥有一条高防IP线路，同时您的账号下还可能拥有多个高防IP实例，因此大多数情况下您的账号都会拥有多条高防IP线路。

在将网站域名添加至高防IP实例进行防护时，您已经为该域名配置至少一条高防IP线路作为转发线路。当您的网站域名配置存在多条高防IP线路作为转发线路时，您需要考虑该网站业务流量的最佳调度方式（即如何将业务流量调度到最优的高防IP线路），提升网站的访问速度和网站接入的高可用性。

DDoS高防IP服务提供两种流量调度方式供您选择。

- 负载均衡

  负载均衡调度方式指按照DNS请求的运营商来源进行响应。例如，来自联通的DNS请求，分配至联通线路的高防IP进行转发；来自电信的DNS请求，则分配至电信线路的高防IP进行转发；来自移动的DNS请求，则分配至移动线路的高防IP进行转发。通过将来自联通的流量调度到联通高防IP线路，来自电信的流量调度到电信高防IP线路，来自移动的流量调度到移动高防IP线路，避免跨网访问。

  如果该网站配置了多条相同运营商的高防IP线路，来自该运营商网内的流量将平均分配至这些相同运营商的高防IP线路。

  负载均衡调度方式为默认的流量调度方式。启用负载均衡方式，将自动开启CNAME自动调度功能，如果某条高防IP线路进入黑洞，将按照 BGP>电信>联通>移动 的线路顺序进行调度。例如，您的网站配置了电信、联通和BGP三条高防IP线路，采用负载均衡的流量调度方式，如果电信高防IP线路被黑洞，流量将自动调度到BGP高防IP线路；如果BGP高防IP线路也被黑洞，将再自动调度到联通高防IP线路。直到已配置的所有高防IP线路都被黑洞时，您的网站业务访问才会中断。

- 优先级

  优先级调度方式指针对所有的DNS请求均回应优先级最高的高防IP线路，即所有流量被调度至当前优先级最高的高防IP线路。当您选择优先级调度方式时，可以编辑高防IP线路的优先级。默认优先级为100，该值越小则表示该高防IP线路优先级越高。

  当优先级最高的高防IP线路被黑洞后，流量将自动调度到优先级次高的高防IP线路。如果优先级次高的高防IP线路存在多条，则按负载均衡方式进行流量调度。

前提条件

确认需要修改的网站域名已经配置接入高防IP实例进行防护。

> 说明:
> 如果您还未将需要配置的网站域名接入高防IP实例，请参考*HTTP*网站接入或*HTTPS*网站接入将您的域名添加至已购买的高防IP实例。

参考以下步骤，修改指定网站域名的业务流量调度方式。

> 说明:
> 建议您先使用测试域名熟悉操作步骤后，再进行实际业务的配置修改。同时，建议您在业务低峰期修改流量调度方式，避免对实际业务产生影响。

1. 登录云盾*DDoS*防护管理控制台，定位到接入 > 网站页面。

2. 定位到需要修改的网站域名配置记录，单击实例与线路区域中流量调度方式右侧的编辑。

3. 在编辑流量调度方式对话框中，选择调度方式，单击确定。

- 负载均衡：流量调度方式默认采用负载均衡方式。负载均衡方式将按照DNS请求的运营商来源进行流量调度，即来自联通的流量将调度到联通高防IP线路、来自电信的流量将调度到电信的高防IP线路、来自其它运营商（如长城宽带）的流量将牵引到BGP高防IP线路。

  说明:
  该网站域名的DNS解析必须通过CNAME记录的方式解析至高防IP服务。

- 优先级：选择优先级调度方式，所有流量将被调度到优先级最高的高防IP线路。

  说明:
  您必须提前为高防IP线路设置优先级。具体设置方法，请参考设置线路优先级。

设置线路优先级

参考以下步骤，为您的高防IP线路设置优先级：

说明:
负载均衡调度方式不受线路优先级影响。只有选择优先级流量调度方式时，高防IP线路的优先级设置才会生效。

1. 登录云盾DDoS防护管理控制台，定位到接入 > 网站页面。
2. 定位到需要设置线路优先级的网站域名配置记录，单击域名信息区域中的回源编辑，打开回源编辑页面。

> **说明:**
> 您也可以单击该网站域名配置记录的实例与线路区域中的编辑，打开回源编辑页面。

3. 将鼠标移至各高防IP线路的优先级处，单击编辑按钮，按照设想的调度方案设置各高防IP线路的优先级。

例如，您想要将业务流量先调度到BGP高防IP线路。当BGP线路被黑洞不可用后，将流量自动调度到电信高防IP线路；如果电信高防IP线路也被黑洞，则将流量调度到联通高防IP线路；当BGP高防IP线路的黑洞解除后，流量自动恢复调度至BGP高防IP线路。

您可以通过将BGP高防IP线路的优先级设置成1、电信高防IP线路的优先级设置成2、联通高防IP线路的优先级不变，并采用优先级的流量调度方式即可满足上述调度方案。

4.2.4 黑洞解封

DDoS高防IP服务提供对进入黑洞的高防IP实例中部分线路的高防IP进行解封的功能，即您可以自行针对某条被黑洞的高防线路的高防IP进行解封操作。

背景信息

说明:

- 每个高防IP服务用户每天拥有三次黑洞解封机会，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黑洞解封次数，当天未使用的解封次数不会累计到下一天。
- BGP线路暂不支持黑洞解封操作。
- 由于黑洞解封涉及阿里云后台系统的风控管理策略，黑洞解封可能失败（解封失败不会扣减您的解封次数）。如果出现未能成功解封的情况，请您耐心等待一段时间后再次尝试。
- 在执行黑洞解封操作前建议您先查看平台自动解封时间，如果您可以接受该自动解封时间，建议您耐心等待。

操作步骤

1. 登录云盾DDoS防护管理控制台。
2. 定位到资产 > 资产列表，找到处于黑洞状态的高防线路，单击防护信息栏中的防护设置，系统将自动跳转至该线路的防护设置页面。

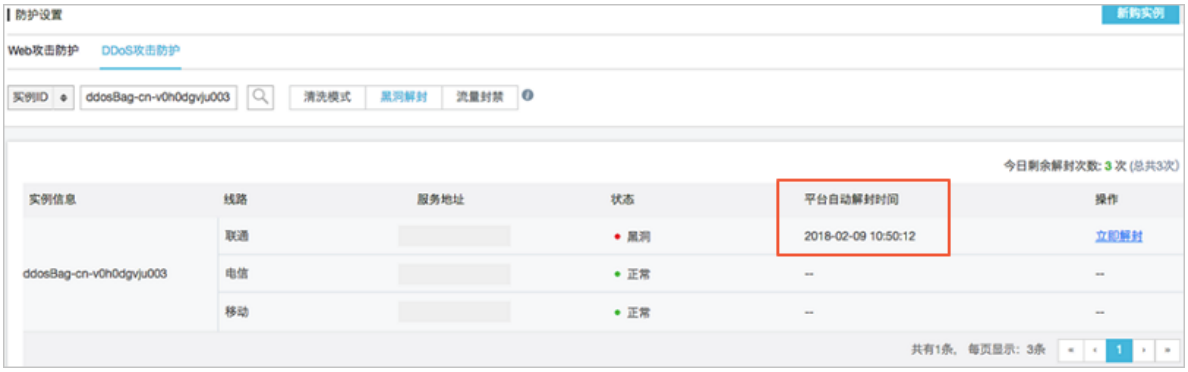
说明:

您也可以定位到防护 > 防护设置 > DDoS攻击防护页面，手动查找需要解封黑洞的高防IP实例线路。

3. 单击黑洞解封，找到处于黑洞状态的高防线路，查看平台自动解封时间。

说明:

如果您可以接受该自动解封时间，建议您耐心等待黑洞状态自动解封。



4. 单击立即解封。

> 说明:
> 如果黑洞解封失败，您会收到失败提示信息，请耐心等待一段时间后再尝试；如果无任何提示信息，则表示解封成功，您可以刷新线路状态确认该高防线路是否已恢复正常。

4.2.5 流量封禁

DDoS高防IP服务支持对高防IP实例中的电信线路实行主动流量封禁，即您可以针对高防电信线路进行流量封禁操作。

背景信息

在您的高防IP实例的电信线路遭受大流量攻击时，您可以通过开启流量封禁功能将特定流量在机房侧丢弃，降低高防电信线路被攻击进入黑洞状态的可能性。由于黑洞涉及攻击流量大小、攻击流量来源区域等多种因素，启用流量封禁可在一定情况下降低被黑洞的概率。

> 说明:
> - 流量封禁功能暂时仅支持电信线路。
> - 每个拥有基础防护带宽为60G或以上电信线路的高防IP实例用户总共拥有最多三次流量封禁操作机会。
> - 您可针对来自非中国大陆地域或中国大陆地域非电信运营商两个区域的流量进行封禁，但不支持将来自这两个区域的流量同时封禁。
> - 单次流量封禁操作最长支持23小时59分、最短5分钟。流量封禁期间，您可以提前手动解除流量封禁。

操作步骤

1. 登录云盾DDoS防护管理控制台。
2. 定位到资产 > 实例列表，选择需要执行流量封禁操作的高防线路，单击防护信息栏中的防护设置，系统将自动跳转至该线路的防护设置页面。

> **说明:**
> 您也可以定位到防护 > 防护设置 > DDoS攻击防护页面，手动查找需要进行流量封禁的高防IP实例线路。

3. 单击流量封禁，选择需要封禁的高防IP实例的电信线路，单击立即封禁。

4. 在流量封禁对话框中，选择封禁区域、设置封禁时长，单击确定。

> **说明:**
> 如果流量封禁失败，您会收到失败提示信息，请根据提示排查后再次尝试；如果未出现任何提示信息，则表示流量封禁已成功，同时列表中将显示本次封禁的区域以及时间范围，且操作栏中的按钮变为解封，单击解封，即可提前解除该线路的流量封禁。

4.3 网络四层防护设置

4.3.1 四层清洗模式设置

DDoS高防IP服务提供IP级别的流量清洗策略调整功能，针对DDoS攻击提供四种四层清洗模式供您选择。

背景信息

 说明:

清洗模式调整目前仅支持电信、联通、移动、海外高防线路，BGP线路暂时不支持清洗策略的调整。在您变更清洗模式后的数分钟内，调整即可生效。

- 宽松模式：采用较大的限速阈值（基本无限制），清洗策略极度宽松。
  - 过滤具有明确的DDoS特征的攻击包（例如，UDP反射攻击包、不符合TCP协议特征的攻击包）
  - 过滤明确的SYN Flood、ACK Flood等攻击
  - 针对访问源IP及目的IP实行非常宽松的限制，主要是进行限速
- 正常模式：默认清洗模式，清洗策略不松不紧。
  - 过滤具有明确的DDoS特征的攻击包（例如，UDP反射攻击包、不符合TCP协议特征的攻击包）
  - 过滤明确的SYN Flood、ACK Flood等攻击
  - 在一定范围内针对访问源IP及目的IP实行限制，主要是进行限速
  - 在特殊情况下，会在一定范围内启用反向探测算法进行过滤
- 攻击紧急模式：针对单个IP的连接进行检查，超过一定连接数的IP将被封禁，清洗策略相对严格。
  - 过滤具有明确的DDoS特征的攻击包（例如，UDP反射攻击包、不符合TCP协议特征的攻击包）
  - 过滤明确的SYN Flood、ACK Flood等攻击
  - 丢弃UDP包
  - 在一定范围内针对访问源IP及目的IP实行限制，进行限速及恶意IP封禁、并针对连接进行限制
- 严格模式：在一定条件下自动启用源认证算法进行过滤，清洗策略严格。
  - 过滤具有明确的DDoS特征的攻击包（例如，UDP反射攻击包、不符合TCP协议特征的攻击包）
  - 过滤明确的SYN Flood、ACK Flood等攻击
  - 丢弃UDP包
  - 在一定范围内针对访问源IP及目的IP实行限制，进行限速及恶意IP封禁、并针对连接进行限制
  - 在一定范围内启用反向探测算法进行过滤。

 说明:

可能存在部分访问端对该算法无法响应，导致一定程度的误杀。

默认情况下，您所购买的高防IP实例采用正常清洗模式，您可以根据实际情况自由调整四层清洗模式。

说明:

BGP线路不支持修改清洗模式。

操作步骤

1. 登录云盾DDoS防护管理控制台。
2. 定位到资产 > 实例列表，选择需要调整清洗模式的高防IP实例，单击防护信息栏中的防护设置，系统将自动跳转至该实例的DDoS攻击防护设置页面。

   说明:

   您也可以定位到防护 > 防护设置 > DDoS攻击防护页面，手动查找需要调整清洗模式的高防IP实例。

3. 单击清洗模式，定位到需要调整清洗模式的线路，单击修改清洗模式。

4. 选择清洗模式，单击确定。

预期结果

清洗模式调整后在数分钟内即可生效。

4.3.2 非网站业务健康检查配置

本文介绍了如何配置高防IP非网站 防护的健康检查规则。

参照以下步骤，来配置高防IP非网站防护的健康检查规则。

1. 登录云盾DDoS防护管理控制台，并前往接入 > 非网站页面。
2. 选择实例并选择高防IP。
3. 选择相应规则，单击其健康检查列下的配置，对健康检查进行配置。默认未开启健康检查。

> **说明:**
> 转发协议为TCP协议时，健康检查方式可选TCP或HTTP。

参数说明

在配置健康检查时，建议您使用默认值。

表 4-1: 四层健康检查

健康检查配置	说明
检查端口	健康检查服务访问后端服务器时的探测端口。默认值为配置监听时指定的后端端口。
响应超时时间	每次健康检查相应的最大超时时间。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。

健康检查配置	说明
检查间隔	进行健康检查的时间间隔。高防集群内所有节点，都会独立、并行地遵循该属性对后端服务器进行健康检查。由于各高防节点的检查时间并不同步，所以，如果从后端某一服务器上进行单独统计，会发现来自高防IP的健康检查请求在时间上没有遵循指定的时间间隔。
不健康阈值	同一高防节点服务器针对同一后端服务器，在健康检查状态为成功时，连续多少次健康检查失败后，状态判定为失败。
健康阈值	同一高防节点服务器针对同一后端服务器，在健康检查状态为失败时，连续多少次健康检查成功，状态判定为成功。

表 4-2: 七层健康检查

健康检查配置	说明
域名和检查路径(仅限HTTP协议)	七层健康检查默认由高防转发系统向该服务器应用配置的缺省首页发起 HTTP HEAD 请求。 · 如果您用来进行健康检查的页面并不是应用服务器的缺省首页，需要指定域名和具体的检查路径。 · 如果您对 HTTP HEAD 请求限定了host字段的参数，您只需要指定检查路径，即用于健康检查页面文件的URI。域名不用填写，默认为后端服务器的IP。
正常状态码	健康检查正常的HTTP状态码。默认值为http_2xx，无法配置。如果HTTP返回状态码非2xx，默认为不健康。
其他参数选项	同四层健康检查参数。

4.3.3 非网站业务DDoS防护策略配置

本文档主要介绍高防IP对于非网站业务提供的DDoS防护策略功能，适用于高防IP的非网站业务的DDoS防护策略优化。

高防非网站业务的DDoS防护策略（以下简称防护策略）是基于IP地址&端口级别 的防护，对于接入高防IP的非网站业务的IP及端口的连接速度、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。

针对非网站业务，您可以通过以下方式配置防护策略：

登录云盾*DDoS*防护管理控制台，在接入 > 非网站页面内，选择高防IP实例，针对某个IP、某个端口，进行DDoS防护策略设置。

说明:

防护策略配置为端口级别。

关于DDoS防护策略配置项详细说明：

DDoS防护策略配置项	说明
虚假源与空连接	虚假源与空连接防护，仅适用于TCP协议规则。
源新建连接限速	单一源IP每秒新建连接，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。
源并发连接限速	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	目的IP及端口每秒最大新建连接数，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	目的IP及端口最大并发连接数，超过限制的链接将被丢弃。
包长度过滤	报文所含payload长度大小，单位为字节(byte)，小于最小长度或大于最大长度的包会被丢弃。

4.3.4 非网站业务会话保持配置

高防IP非网站 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个后端服务器上。

操作步骤

1. 登录云盾DDoS防护管理控制台，并前往接入 > 非网站页面。
2. 选择实例并选择高防IP。
3. 选择规则，单击其会话保持列下的配置。会话保持配置为端口级别。
4. 设置超时时间后，单击保存。

4.4 实例管理

4.4.1 启用停用某条线路

本文介绍了在网站转发中如何取消某条线路解析，或者取消某条线路转发配置。

取消线路解析

> 说明:
> 此操作只适用于使用网站配置中产生的CNAME进行域名解析的用户，请确认您的网站使用高防提供的CNAME方式接入。

参照以下步骤，来取消某条线路解析。

1. 登录云盾DDoS防护管理控制台，并前往接入 > 网站页面。
2. 选择需要修改的网站实例，单击其域名信息下的回源编辑。
3. 在高防IP/域名解析开关列下，选择需要取消解析的某条线路，并单击其启停开关，取消该解析。

取消某条线路的解析后，网站流量将不再从某条线路进入。

删除线路转发配置

> 说明:
> 在操作前，请确认访问网站流量从已启用的线路进入。如果您使用高防网站配置提供的CNAME接入，请确认是否已取消某条线路解析，即移除了需要删除线路的CNAME解析。

参照以下步骤，来删除某条线路转发。

1. 登录云盾DDoS防护管理控制台，并前往接入 > 网站页面。
2. 选择需要修改的网站实例，单击其域名信息下的回源编辑。
3. 在操作 列下，单击编辑线路。
4. 在编辑线路页面，选择需要删除某条线路转发规则的线路，单击停用。

说明:

选择停用某条线路后，请充分确认访问网站流量不从停用的线路进入。

4.4.2 调整弹性防护带宽

您可以在控制台实时调整高防IP实例的弹性防护带宽。

背景信息

高防IP实例启用弹性防护带宽后，当攻击峰值超出保底防护带宽（即基础防护）时，高防IP会根据您设置的弹性防护带宽值进行防护。假设高防IP实例的基础防护带宽是20G，弹性防护带宽是30G，则当攻击峰值超过20G时会触发弹性带宽防护，该实例的实际防护能力达到30G。

在触发弹性防护（攻击峰值超过保底防护带宽）时，弹性防护根据当天实际发生的攻击峰值生成后付费账单。当天未触发弹性防护时，不产生费用。您可以根据实际业务情况实时调整弹性防护带宽。

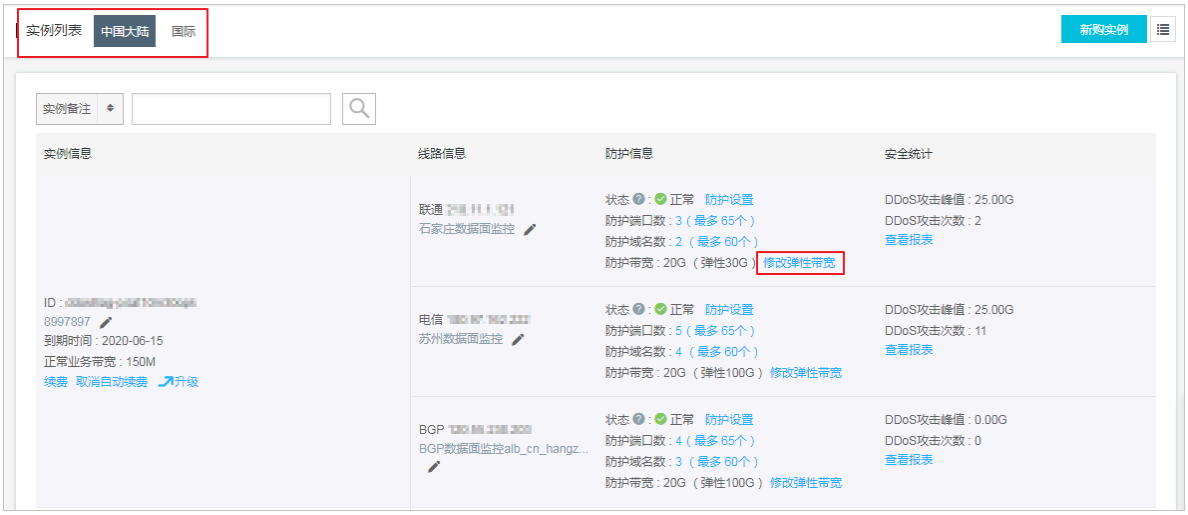
关于弹性带宽的价格，请参考高防IP价格详情页。

操作步骤

1. 登录云盾DDoS防护管理控制台。
2. 前往资产 > 实例列表页面，在页面上方选择实例所在地区（中国大陆、国际）。
3. 选择要操作的实例和线路，在其防护信息列下，单击修改弹性带宽。

说明:

不同线路的弹性后付费价格不同，具体请参考高防IP价格详情页。



4. 在修改弹性带宽对话框中，选择合适的带宽值，单击确定。

说明:

弹性带宽修改后在次日生效。

4.4.3 更换 ECS IP

若您的源站IP已暴露，建议您使用阿里云提供的IP，防止黑客绕过高防直接攻击源站。您可以在高防IP管理控制台更换后端ECS的IP，每个账号最多可更换10次。

操作步骤

1. 登录云盾DDoS防护管理控制台。
2. 定位到接入 > 网站，单击更换ECS IP。

:

更换ECS IP会使您的业务暂时中断几分钟，建议您在操作前先备份好数据。

3. 更换ECS IP需要将ECS停机，若您已将需要更换IP的ECS停机，请直接跳转到步骤4。在更换ECS IP对话框，单击前往ECS，在ECS管理控制台将需要更换IP的ECS实例停机。
   a) 在实例列表中找到目标ECS实例，单击其实例ID。
   b) 在实例详情页，单击停止。
   c) 选择停止方式，并单击确定。

   > 说明:
   > 停止ECS实例是敏感操作，稳妥起见，需要您输入手机校验码。

   d) 等待ECS实例状态变成已停止。
4. 返回更换ECS IP对话框，输入ECS实例ID，并单击下一步。
5. 确认当前ECS实例信息准确无误（尤其是ECS IP）后，选择更换IP后 是否立刻重启ECS，并单击释放IP。
6. 成功释放原IP后，单击下一步，为该ECS实例重新分配IP。
7. ECS IP更换成功，单击确认，完成操作。

   > 说明:
   > 更换IP成功后，请您将新的IP隐藏在高防后面，不要对外暴露。

4.4.4 管理抗D包

抗D包是高防IP实例用户的一项增值服务，帮助提升高防IP实例的弹性防护能力。

什么是抗D包?

抗D包是高防IP实例用户的一项增值服务，帮助提升高防IP实例的弹性防护能力。有别于高防IP实例本身所具备的按量后付费模式的弹性防护能力，抗D包提供的是按次数消耗的单个自然日内指定数值（最大）的弹性防护能力。当攻击流量超过高防IP实例的保底带宽时，系统自动启用所绑定的抗D包的弹性防护能力进行防护，并扣除该抗D包的防护次数，且该自然日内的所产生的弹性防护流量（不超过该抗D包防护规格）将不会产生后付费的弹性防护费用。

> 说明:
> 如果遭受的攻击流量超出抗D包的防护规格，超出最大防护能力的攻击流量仍需要高防IP实例本身的弹性防护能力进行防护，并根据超出部分的弹性防护流量计算后付费的弹性防护费用。

例如，您将一个300Gb防护规格的抗D包绑定至指定高防IP实例的电信线路IP，该电信线路IP的弹性防护带宽自动调整至300Gb。当该IP遭受大于高防IP实例保底防护带宽的DDoS攻击时，所绑定的抗D包的可用次数将被扣减一次（一个自然日内最多只会扣减一次），且当日内该电信线路

IP所遭受的300Gb内的攻击防护流量将不会产生弹性防护费用。如果当日内遭受的DDoS攻击超过300Gb，超出300Gb部分的攻击仍将产生弹性防护费用。

当抗D包的可用次数被扣减至0后，该线路的弹性防护带宽将自动恢复至绑定抗D包前所设置的弹性防护值。

由于抗D包按照自然日消耗使用次数，因此更适合用于一日内遭受长时间持续DDoS攻击的防护场景。对于短时间内遭受的大流量DDoS攻击（攻击峰值超过抗D包防护规格）的场景，建议您仍然通过高防IP实例本身的弹性防护能力进行防护。

 说明:

抗D包目前仅支持绑定高防IP实例中电信或联通线路IP。

如何获得抗D包?

目前，抗D包仅以用户增值服务的方式赠送。

在您首次购买20Gb-200Gb保底防护带宽规格的高防IP实例并完成支付后，如果您的高防IP实例遭受到超过保底防护能力的攻击，您将获赠拥有3次可用防护次数的300Gb规格的抗D包。

抗D包发送成功后，您将收到短信提醒，请及时前往DDoS高防管理控制台的增值服务页面领取您的抗D包。

 说明:

如抗D包发送至您的增值服务十天后仍未被领取，该抗D包将自动失效，请务必及时领取。

如何使用抗D包?

在增值服务中成功领取抗D包后，您可以在DDoS高防管理控制台 > 资产 > 抗D包页面查看您所拥有的抗D包。

参考以下操作步骤，将您的抗D包绑定至高防IP实例中的电信或联通线路IP：

 注意:

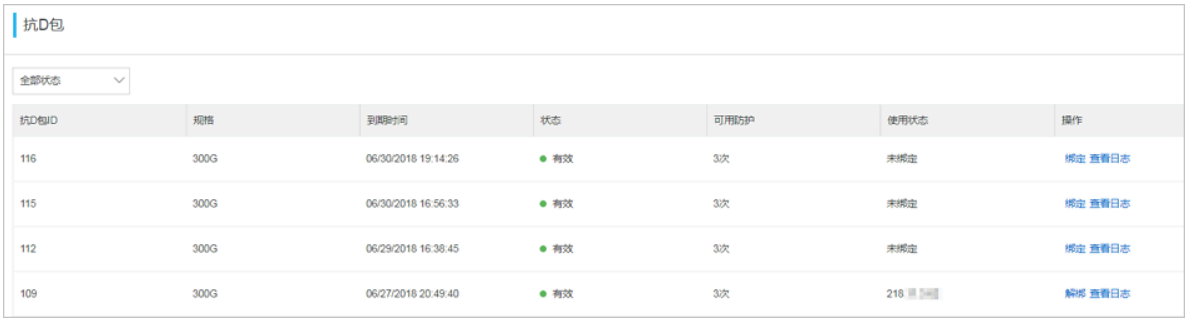
将抗D包绑定至高防IP实例中的电信或联通线路IP后，该IP当日内（自然日）所遭受的抗D包防护规格内的攻击防护流量将不会产生弹性防护费用。

- 无论DDoS攻击是否在绑定抗D包后发生，该自然日内所有超出高防IP实例保底防护能力所产生的弹性防护流量（不超过该抗D包防护规格）费用都将被免除。即在该自然日内，只要所遭受的DDoS攻击流量不超过该抗D包的防护规格，将不会产生弹性防护费用的后付费账单。
- 非该自然日内产生的超出高防IP实例保底防护能力所产生的弹性防护流量将正常计费并生成后付费账单。

1. 登录云盾DDoS防护管理控制台。
2. 定位到资产 > 抗D包页面，选择抗D包，单击绑定。
3. 输入您要绑定的高防IP实例的电信或联通线路IP，单击确定。

   绑定成功后，抗D包即生效。单击解绑，可以随时解除绑定关系。

> **说明:**
> 单击查看日志，您可以查询该抗D包的绑定、解绑等操作日志。



4.5 统计报表

4.5.1 查看安全概览报表

DDoS高防IP的安全概览报表，通过丰富的图文报表将攻防过程中的数据完全透明化，帮助您全面了解业务的DDoS攻防情况。同时，这些DDoS攻防过程的报表数据可满足您年度安全报告、DDoS攻击案件取证/溯源、DDoS攻击态势分析等需求。

背景信息

DoS攻防过程的报表数据可满足您年度安全报告、DDoS攻击案件取证/溯源、DDoS攻击态势分析等需求。

> **说明:**
> 安全概览报表的数据最长支持保存一年。

> **注意:**
> 2018年9月27日，DDoS高防IP新安全概览报表功能开启全面公测。公测期间，用户默认最长可查看近一年的攻防数据。

操作步骤

1. 登录云盾DDoS防护管理控制台。
2. 定位到统计 > 概览，查看安全概览报表。概览报表分非网站和网站进行展示。

- 非网站业务：非网站业务安全概览报表主要展示IP和端口级别的流量、连接和访问来源分布等信息。

  a. 单击选择非网站页签，选择想要查看的DDoS高防IP实例和高防IP，单击确定。

  > 说明：
  > 如果您拥有的高防IP实例和IP较多，建议您通过攻击流量峰值或高防入流量峰值排名选择攻击流量大或高防入流量高的IP，进行相关报表数据的查询和分析，提升查询效率。

  b. 设置查询时间范围，单击确定。

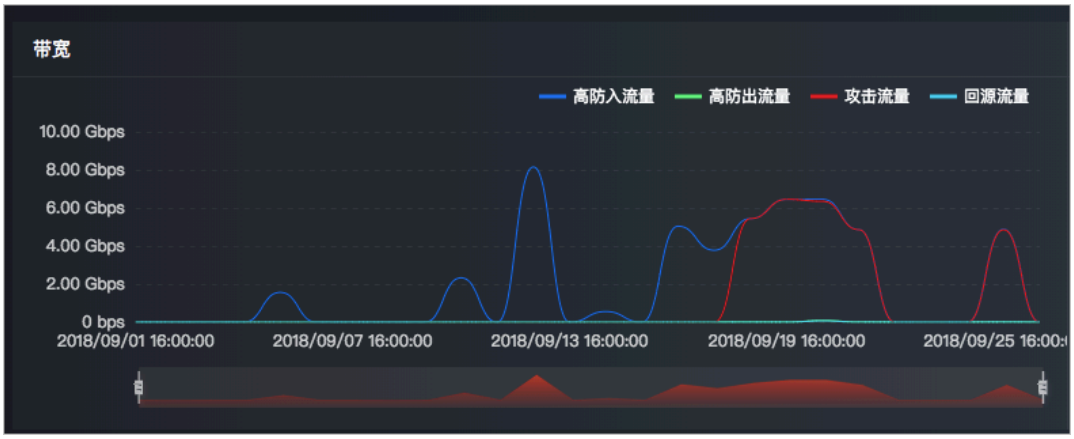
  c. 在安全概览报表中，您可以看到以下信息：

  - 高防入流量峰值：查询时间范围内指定高防IP接收到的流量最大值。
  - 高防出流量峰值：查询时间范围内源站服务器响应用户客户端的业务流量最大值。
  - 攻击流量峰值：查询时间范围内被高防成功清洗的攻击流量最大值。
  - 回源流量峰值：查询时间范围内经过高防清洗后，转发回源到源站服务器的业务流量最大值。

  > 说明：
  > 如果您选择多个高防IP，上述流量峰值将显示查询时间范围内所选择的高防IP对应的流量数据的最大值。

- 流量趋势图： 高防入流量、高防出流量、攻击流量和回源流量在查询时间范围内的流量趋势情况。如果您只选择单个高防IP进行查询，您可以选择设置具体端口，查看指定端口的高防出流量和回源流量趋势信息。

  说明:
  将鼠标移至趋势图上可以查看该时间节点具体的高防入流量、高防出流量、攻击流量和回源流量的最大值。



- DDoS事件：查询时间范围内的DDoS攻击事件的详细情况。DDoS攻击事件分为四种状态：清洗中（无结束时间）、清洗结束（有结束时间）、黑洞中（无结束时间）、黑洞结束（有结束时间）。

  说明:
  将鼠标移至具体DDoS事件记录上，可查看所遭受的攻击类型、被攻击IP和累计攻击流量。单击DDoS事件记录，可查看攻击源IP信息。

- 攻击流量分布：查询时间范围内DDoS攻击流量的分布情况。快速确定攻击流量的来源分布，可有效辅助您进行下一步的安全防护决策。例如，针对性地封禁海外流量、封禁指定区域IDC的流量等。

  说明：
  单击查看攻击源IP，可查看查询时间范围内攻击流量TOP100的攻击源IP。

- 连接数及连接数分布：只有选择单个高防IP时，才会展示该高防IP的连接数及其分布情况，包括并发连接、新建连接等；如果您选择查询多个高防IP，则连接数和连接数分布信息将无法显示。

  说明：
  您可以选择指定端口的连接数据进行展示。

- 网站业务：网站业务安全概览报表主要展示域名的各类请求数据。

  a. 单击选择网站页签，选择想要查看的域名，单击确定。

  > 说明：
  > 在域名列表中您可以自由选择所有已接入防护的域名。域名支持以攻击或总请求数进行排名，帮助您快速确定需要查看的域名信息，提升查询效率。

  b. 设置查询时间范围，单击确定。

  c. 在安全概览报表中，您可以看到以下信息：

  - 用户到高防请求次数：查询时间范围内针对所选择的域名，用户到高防的请求总数。
  - 回源请求次数：查询时间范围内针对所选择的域名的源站接收到的请求总数。
  - 攻击请求次数：查询时间范围内针对所选择的域名的攻击请求总数。

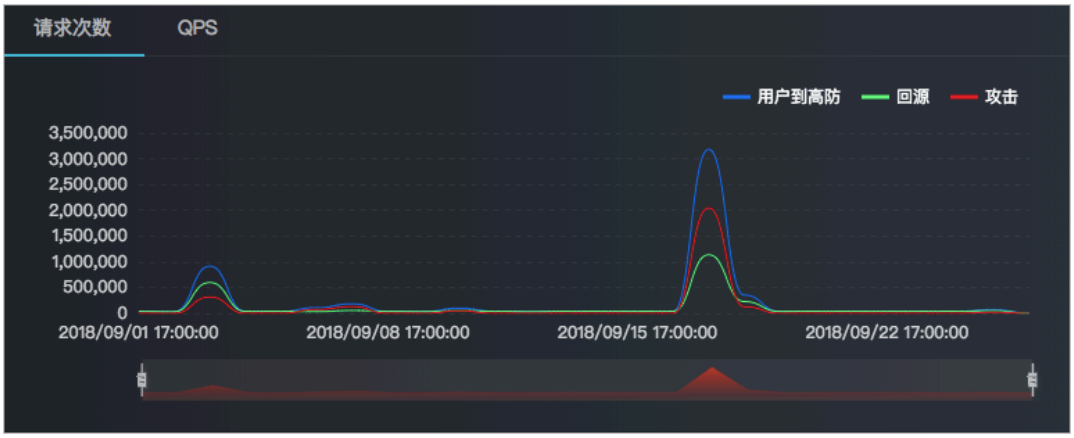
说明:

如果您选择多个域名，上述请求次数将显示查询时间范围内所有已选择域名的汇总值。

- **请求次数及QPS趋势图：请求次数是一定时间间隔内累积的请求次数趋势，具体时间间隔取决于查询时间范围的大小；QPS是查询时间范围内每秒请求次数趋势。趋势图主要展示用户到高防、回源和攻击三个数据指标。**

说明:

单击请求次数或QPS进行切换。



- **CC事件：查询时间范围内所有CC攻击事件信息。**

说明:

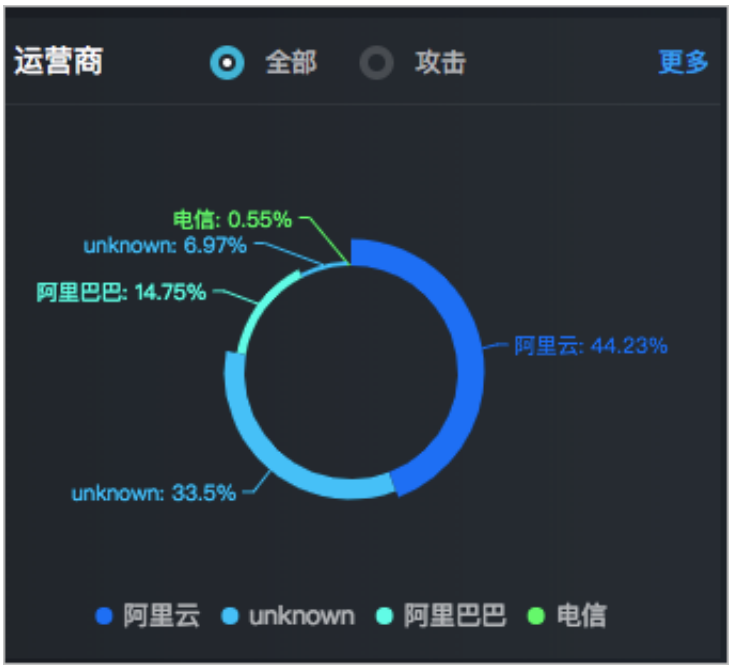
将鼠标移至具体CC攻击事件记录上，可查看被攻击域名和攻击峰值。单击CC攻击事件记录，可查看攻击源IP信息。

- 全部请求和攻击请求分布：查询时间范围内全部请求和攻击请求的分布情况。快速确定网站CC攻击请求的来源分布，可有效辅助您进行下一步的安全防护决策。例如，针对性地封禁海外流量、封禁指定区域IDC的流量等。

> **说明:**
> 单击查看访问源IP或查看攻击源IP，可查看查询时间范围内请求次数TOP100的访问源IP或攻击源IP。

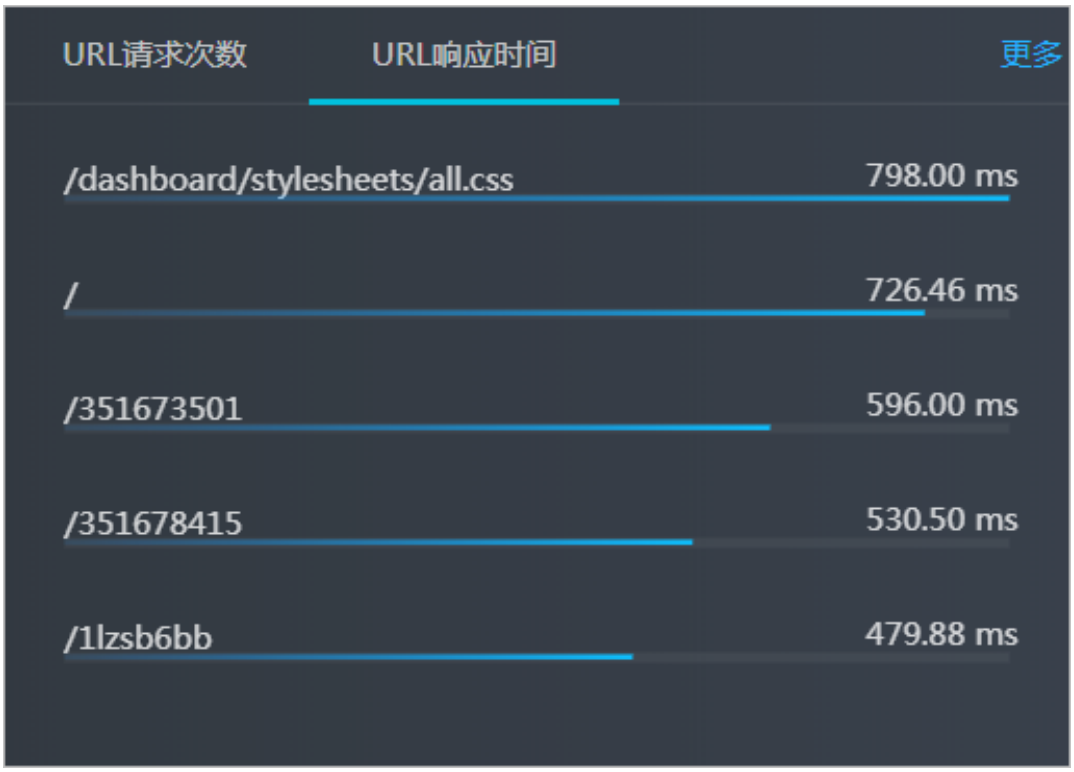
- 响应码趋势分布：查询时间范围内用户到高防或高防到源站的响应码趋势分布情况。当网站访问出现异常时，可以基于响应码数据快速判断问题是发生在高防，还是源站。

- 运营商分布：查询时间范围内全部请求或攻击请求的运营商分布情况。



- URL请求次数：查询时间范围内URL被请求次数排名。单击更多，可查看完整的URL请求次数排名情况。

- URL响应时间：查询时间范围内URL响应时间排名。单击更多，可查看完整的URL响应时间排名情况。

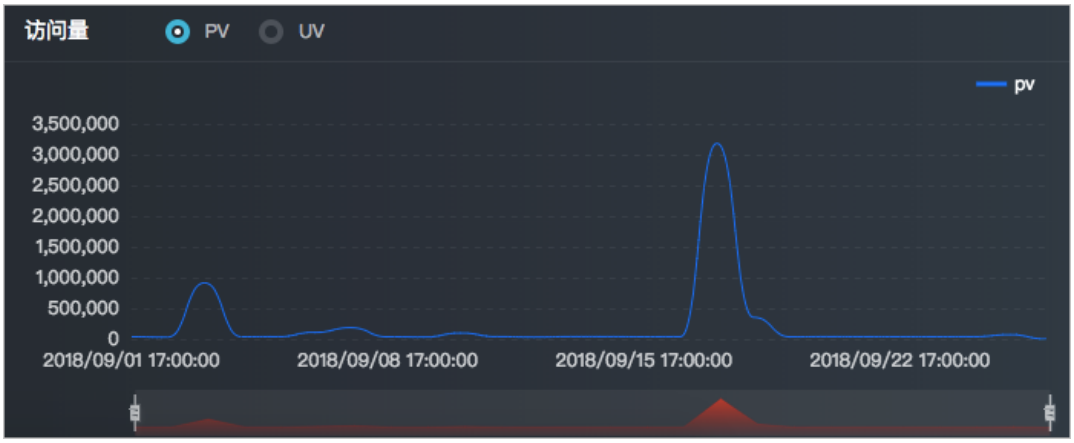


- 浏览器分布排名：查询时间范围内请求来源的浏览器分布排名。单击更多，可查看完整的浏览器排名情况。

- **协议类型分布：查询时间范围内HTTP协议和HTTPS协议的请求峰值和累计请求次数。**

- **访问量趋势图：查询时间范围内域名的访问量（PV）和用户量（UV）趋势信息。**

> **说明:**
> **用户量（UV）趋势信息暂时仅支持暂选择单个域名进行展示。**



4.5.2 查看安全报表

将您的业务接入高防IP防护后，您可以通过查看安全报表了解相关防护信息。

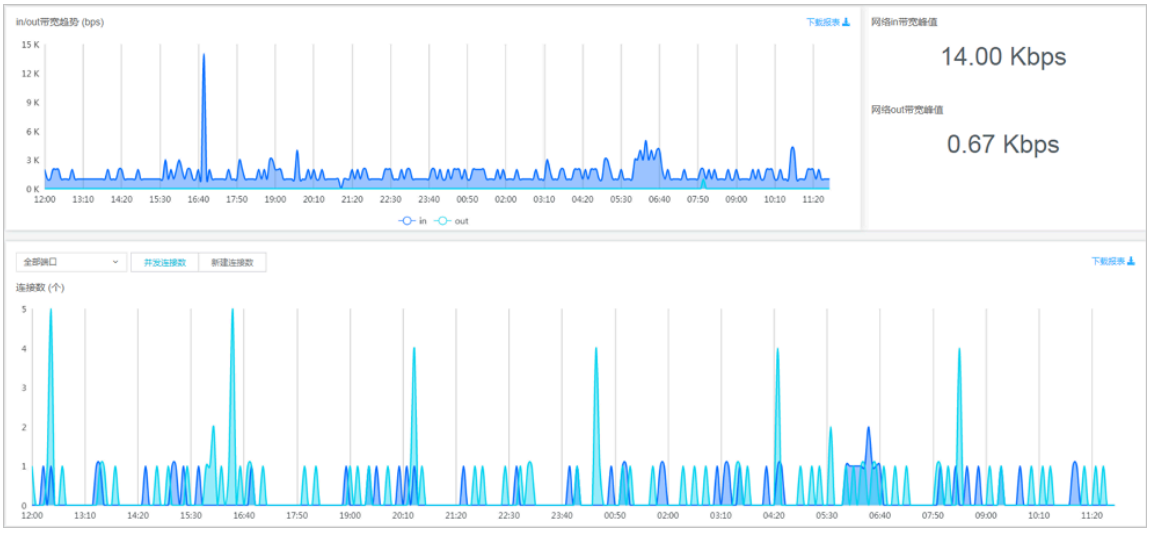
操作步骤

1. 登录 云盾DDoS防护管理控制台。
2. 定位到统计 > 安全报表。
3. 在安全报表页面，选择业务、DDoS攻击防护、CC攻击防护页签，选择高防实例、高防IP或者防护域名，单击查询按钮，查看相关报表。

> **说明:**
> 所有报表均可以设置开始和结束时间作为查询条件。您也可以在快速查询中选择时间范围，查看截至当前时间该段时间范围的数据。

- 业务

  在业务报表中，您可以查看所选择时间范围内的In/Out带宽流量的趋势及新建连接数或并发连接数的趋势。同时，您还可以查看该时间范围内的网络进/出方向的带宽流量峰值。



- DDoS攻击防护

  在DDoS攻击防护报表中，您可以查看到网络接收/攻击流量趋势、攻击类型及详细的DDoS攻击记录。

- CC攻击防护

  在CC攻击防护报表中， 您可以查看所防护域名的QPS次数统计及详细的CC攻击记录。

4.5.3 查看业务遭受的攻击情况

当收到DDoS攻击提醒短信或发现业务出现异常时，您需要快速了解攻击或业务情况，包括攻击类型、流量大小、当前防护效果等。在掌握足够的信息后，您才可以采取正确的处理方式，第一时间保障业务正常。

DDoS高防IP管理控制台的安全报表提供丰富的信息帮助您快速了解当前业务或攻击情况。

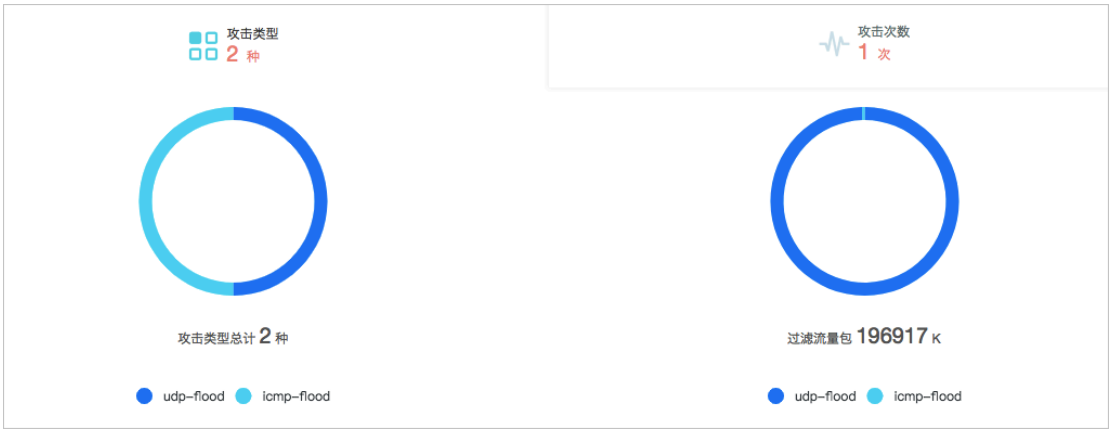
1. 登录云盾DDoS防护管理控制台。
2. 定位到统计 > 安全报表页面，单击DDoS攻击防护页签，选择实例和高防IP，设置查询时间区间，查看是否存在网络流量型攻击。

   - 您可以通过快速查询选择24小时查看当前遭受攻击情况，包括所选择的高防IP的网络接收流量和网络攻击流量趋势。当遭受网络流量型攻击时，在网络流量趋势图中可以明显看到网络攻击流量的峰值及攻击大小。

- 您可以通过单击攻击类型和攻击次数页签查看攻击详情。
  - 攻击次数：查看该时间段内所遭受的攻击次数，以及攻击的开始和结束时间、持续时长、攻击类型和清洗结果。通过单击查看攻击源IP可以查看发起攻击的源IP，同时您可以下载相关信息用于攻击溯源并作为报警证据。

    说明:
    如果攻击持续时间比较短，可能出现查看不到攻击源IP的情况。

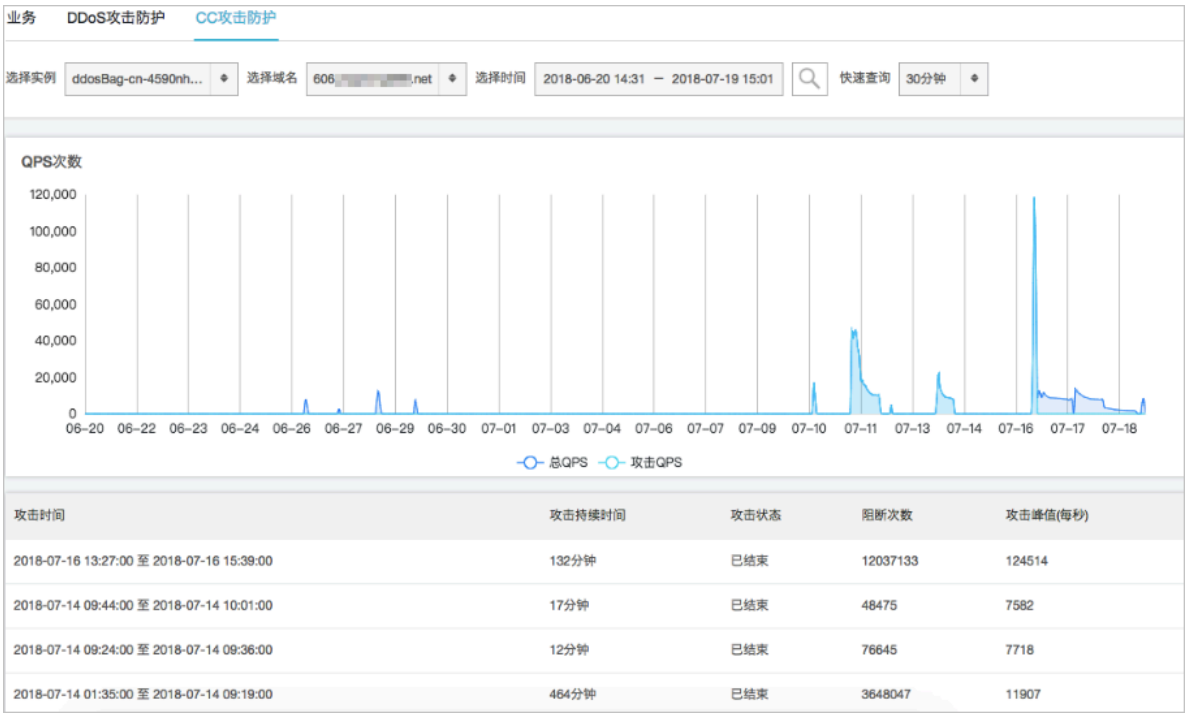
  - 攻击类型：查看该时间段内检测到的攻击类型，以及各攻击类型的流量清洗报文数量，帮助辨别当前流量型攻击的攻击类型分布情况。



3. 定位到统计 > 安全报表页面，单击CC攻击防护页签，选择实例，选择网站域名，设置查询时间区间，查看是否存在网站业务CC攻击。

> **说明:**
> 查看网站业务是否遭受CC攻击，需要确认您的网站业务已添加至DDoS高防的网站域名配置中。

您可以通过快速查询选择24小时查看网站域名的QPS趋势图。您可以观察总QPS值是否远高于您正常情况下的访问量（QPS），并查看攻击QPS是否有数值且数值巨大。如果存在CC攻击，高防会记录下攻击的开始时间、结束时间、攻击持续时间、攻击状态、阻断次数和攻击峰值等信息。



攻击时间	攻击持续时间	攻击状态	阻断次数	攻击峰值(每秒)
2018-07-16 13:27:00 至 2018-07-16 15:39:00	132分钟	已结束	12037133	124514
2018-07-14 09:44:00 至 2018-07-14 10:01:00	17分钟	已结束	48475	7582
2018-07-14 09:24:00 至 2018-07-14 09:36:00	12分钟	已结束	76645	7718
2018-07-14 01:35:00 至 2018-07-14 09:19:00	464分钟	已结束	3648047	11907

攻击处理建议

通过上述方法对您的业务情况和所遭受的攻击情况掌握足够的信息后，您可以参考以下方式进行处理。

- 如果在DDoS攻击防护报表或CC攻击防护报表中已查看到攻击日志，但是业务仍然无法正常访问，您可能需要调整清洗模式来提升清洗效果。

  您可以登录云盾DDoS防护管理控制台，在防护 > 防护设置页面调整清洗模式。

  - 如果是网络流量型攻击，您可以调整指定高防实例线路的清洗模式来应对不同的DDoS攻击类型。

    > **说明:**
    > 关于各四层清洗模式的清洗效果，查看四层清洗模式设置。

  - 如果发现您的高防IP已经被黑洞，您可以通过黑洞解封功能快速解除高防IP的黑洞状态。

- 如果您业务的用户访问主要集中在中国大陆地域，您可以考虑使用流量封禁功能来暂时封禁来自海外的访问流量，压制大流量攻击的规模。
- 如果是网站CC攻击，您可以通过调整被攻击网站域名的清洗模式来应对不同的CC攻击类型。

> 说明:
> 关于各七层清洗模式的清洗效果，查看*HTTP(S) Flood*攻击防护设置。

· 如果在DDoS攻击防护报表或CC攻击防护报表中未查看到任何攻击，但业务仍然无法正常访问，参考以下处理方式。

- 如果是七层网站业务，建议您开启全量日志功能，通过查看七层网站业务的访问日志进一步分析访问问题。例如，发现某个网址访问量特别大的情况，您可以通过CC自定义规则针对该网址进行防护。

> 说明:
> 关于全量日志功能，查看全量日志。

- 如果是四层业务存在大面积用户访问问题，建议您先检查源站服务器（例如，连接数、CPU负载、内存使用率、服务器出口带宽负载情况等），再逐步排查高防到源站服务器的网络接入情况、以及用户侧到高防的网络接入情况等。

4.5.4 配置DDoS事件告警通知

您可以在消息中心管理控制台上，配置高防 IP 服务告警通知方式。

操作步骤

1. 登录 消息中心管理控制台。
2. 定位到消息接收管理 > 基本接收管理，单击消息接收人管理。
3. 在消息接收人管理页面，单击新增消息接收人以添加联系人，或者单击已有联系人操作列下的修改/删除以执行相关操作。
4. 返回基本接收管理页面，在消息类型下勾选安全消息 > 云盾安全消息通知，勾选相应通知方式（站内信、邮箱和短信），并单击消息接收人列下的修改来选择消息接收人。

预期结果

设置完成后，您选择的消息接收人将通过已选择的通知方式，收到高防 IP 服务相关的告警通知。

4.6 日志查询

4.6.1 操作日志

您可以在云盾DDoS防护管理控制台操作日志页面，查看相关的操作日志。

说明:

操作日志只记录最近30天中的重要操作。

操作日志内容	支持情况	备注
ECS更换IP日志	支持	-
CNAME调度日志	支持	-
黑洞解封操作日志	支持	BGP线路不支持黑洞解封。
流量封禁/解封操作日志	支持	目前只有基础防护带宽在60G以上的高防IP实例的电信线路支持流量封禁操作。
四层清洗模式变更操作日志	支持	对于四层清洗模式，目前提供四种强度模式供选择。BGP线路暂不支持修改四层清洗模式。
CC防护模式变更操作日志	支持	对于CC防护模式，目前提供四种强度模式供选择。
弹性防护带宽变更操作日志	支持	-

4.6.2 全量日志

超过80%的DDoS攻击都会混合HTTP攻击，而其中混合的CC攻击尤其隐蔽，因此通过日志对访问和攻击行为进行即时分析研究、附加防护策略就显得尤其重要。

目前，阿里云DDoS高防IP服务的网站访问日志（包含CC攻击日志）已经与日志服务联动，为您提供实时分析与报表中心功能。

日志服务实时采集接入高防IP防护的网站业务的访问日志、CC攻击日志，并对采集到的日志数据进行实时检索与分析，以仪表盘形式展示查询结果。

启用全量日志功能

参考以下操作步骤，为您需要开启全量日志功能的网站域名启用该功能：

> **说明：**
> 启用高防IP服务的全量日志功能将按照日志服务的收费项进行计费，未产生日志数据不会产生任何费用。日志服务采用按量计费模式，同时高防IP的全量日志功能拥有一定量的专属免费额度。

高防IP的全量日志服务费用主要根据所导入的日志量以及日志存储的时间两个主要因素进行计算。当前，高防IP的全量日志服务提供100GB/天的日志一次性导入量和三天的免费日志存储时间。同时，基于日志的查询分析、统计报表和报警等功能均不会产生任何额外费用。

例如，您开启全量日志功能的网站业务每天有6千万条日志、日志的存储周期为三天，总日志量约为96GB/天（平均每条日志约1600字节左右），在专属免费额度范围内，将不产生任何额外费用。如果您的网站业务的访问日志超过该量级则可能产生后付费，具体收费标准和计费方式参考*DDoS高防日志-费用说明*。

1. 登录*云盾DDoS防护管理控制台*，定位到日志 > 全量日志页面。
2. 选择您需要开启高防IP全量日志采集功能的网站域名，单击状态开关启用全量日志功能。

启用全量日志功能后，您可以在全量日志页面对采集到的日志数据进行实时查询与分析、查看或编辑仪表盘、设置监控告警等。关于高防IP服务的日志分析与日志报表功能，参考*DDoS*高防日志-日志报表与*DDoS*高防日志-日志分析。

全量日志功能应用场景

通过启用DDoS高防IP服务的全量日志功能，可以满足您在以下访问日志分析场景中的需求。

- 排查网站访问异常

  配置日志服务采集DDoS高防日志后，您可以对采集到的日志进行实时查询与分析。使用SQL语句分析网站访问日志，对网站的访问异常进行快速排查和问题分析，并查看读写延时、运营商分布等信息。

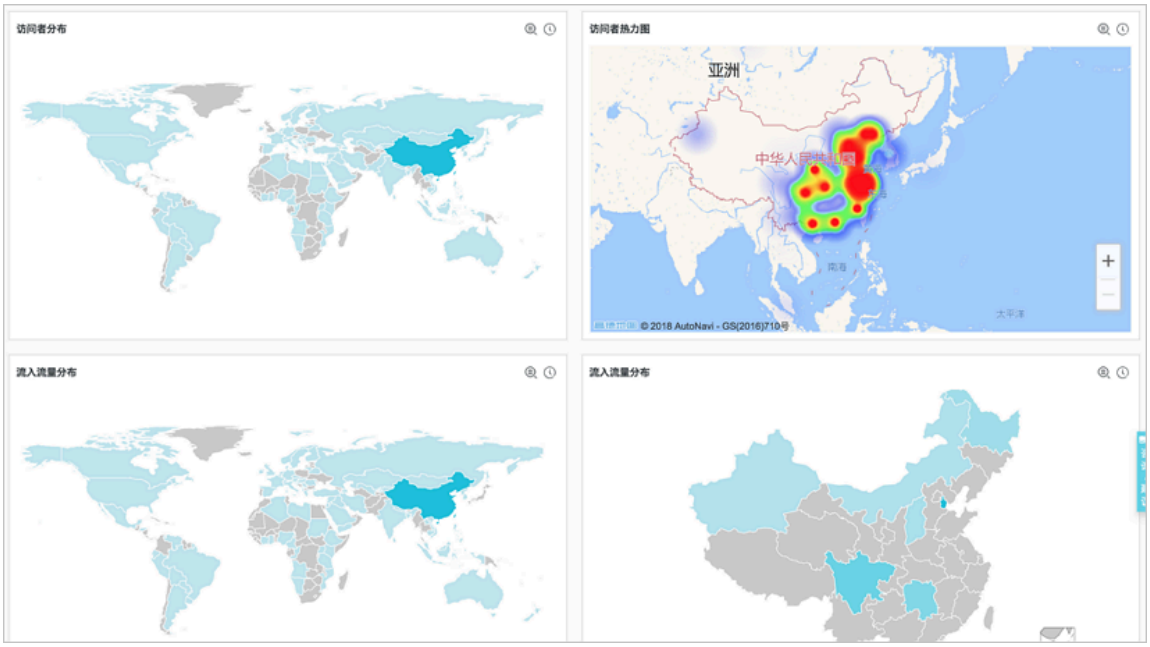
  例如，通过以下语句查看网站访问日志：

  ```
  __topic__: DDoS_access_log
  ```

- 追踪CC攻击者来源

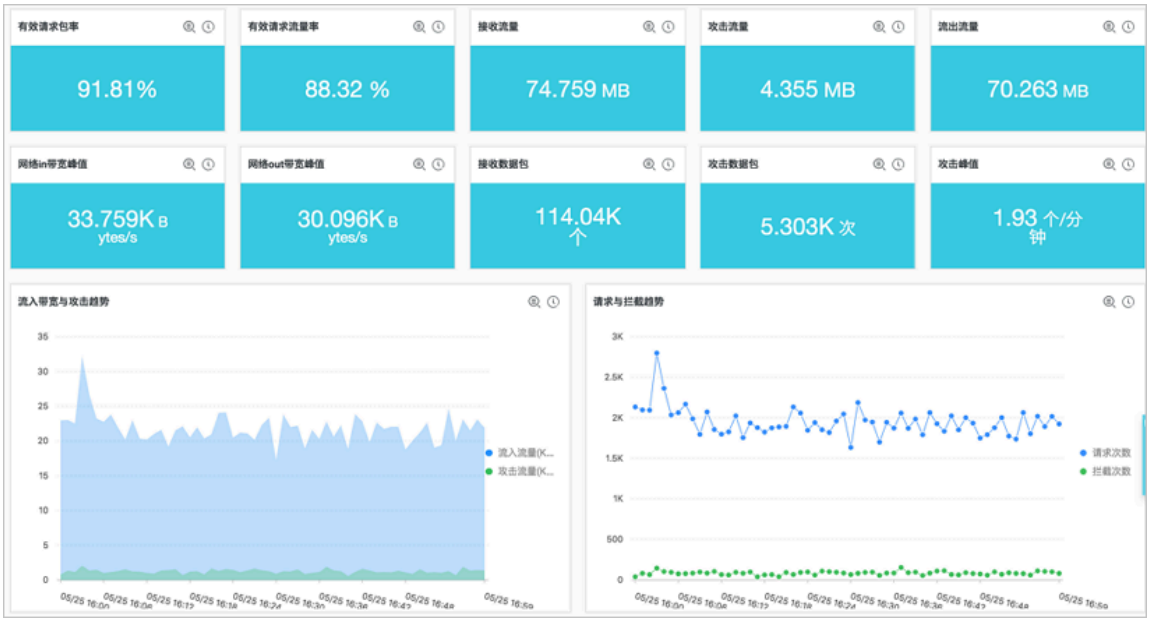
  - 例如，通过以下语句分析DDoS访问日志中记录的CC攻击者国家分布：

    ```
    __topic__: DDoS_access_log and cc_blocks > 0| SELECT ip_to_country
    (if(real_client_ip='-', remote_addr, real_client_ip)) as country,
    count(1) as "攻击次数" group by country
    ```



- 例如，通过以下语句查看访问PV：

```
__topic__: DDoS_access_log | select count(1) as PV
```



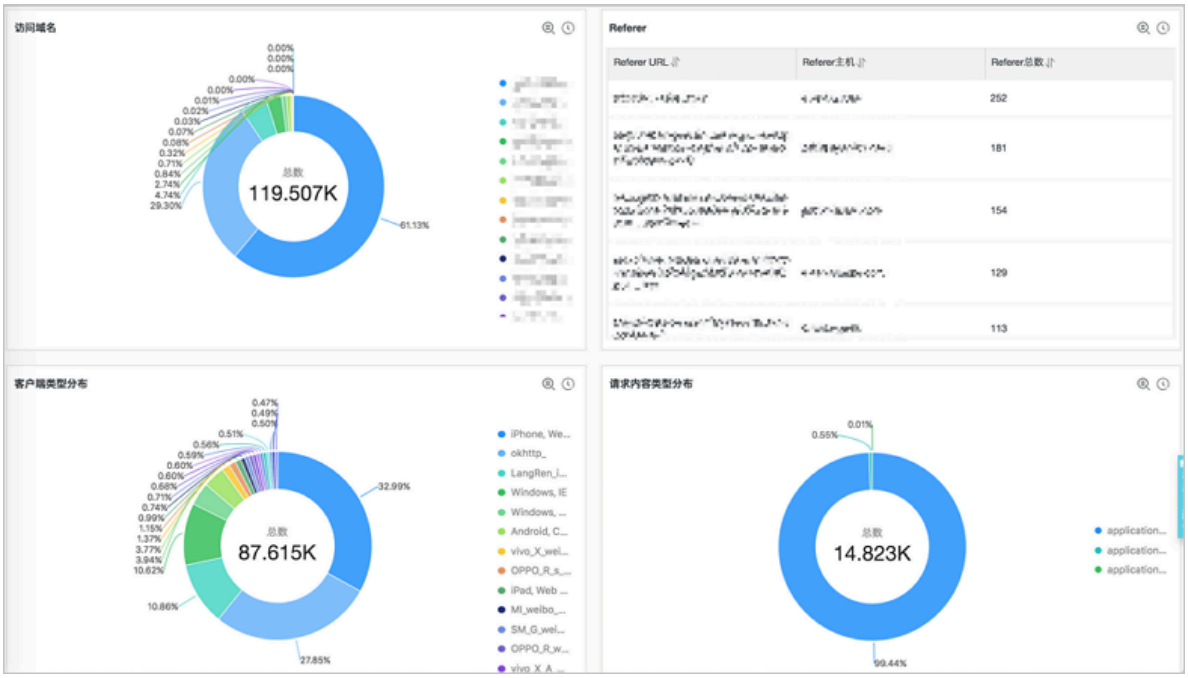
· 网站运营分析

网站访问日志中实时记录网站访问数据，您可以对采集到的访问日志数据进行SQL查询分析，得到实时的访问情况，例如判断网站热门程度、访问来源及渠道、客户端分布等，并以此辅助网站运营分析。

例如，查看来自各个网络服务提供商的访问者流量分布：

```
__topic__: DDoS_access_log | select ip_to_provider(if(real_client_ip
='-', remote_addr, real_client_ip)) as provider, round(sum(request_le
```

```
ngth)/1024.0/1024.0, 3) as mb_in group by provider having ip_to_prov
ider(if(real_client_ip='-', remote_addr, real_client_ip)) <> '' order
by mb_in desc limit 10
```



4.7 安全服务

4.7.1 开通高防安全服务授权

通过高防安全专家服务，您将获得阿里云安全服务专家和第三方安全专家针对您业务场景的提供的高防产品安全服务，帮助您基于业务实际情况更好地使用高防产品功能，保障业务的网络应用安全。

背景信息

安全专家可以为您提供高防中的域名防护咨询服务，也会对您的业务日志数据进行深度分析，有针对性地为您提供高防防护配置的相关建议等。

购买高防产品安全服务后，您需要开通服务授权，允许阿里云安全服务专家和第三方安全专家通过阿里云安全服务平台为您提供产品服务。

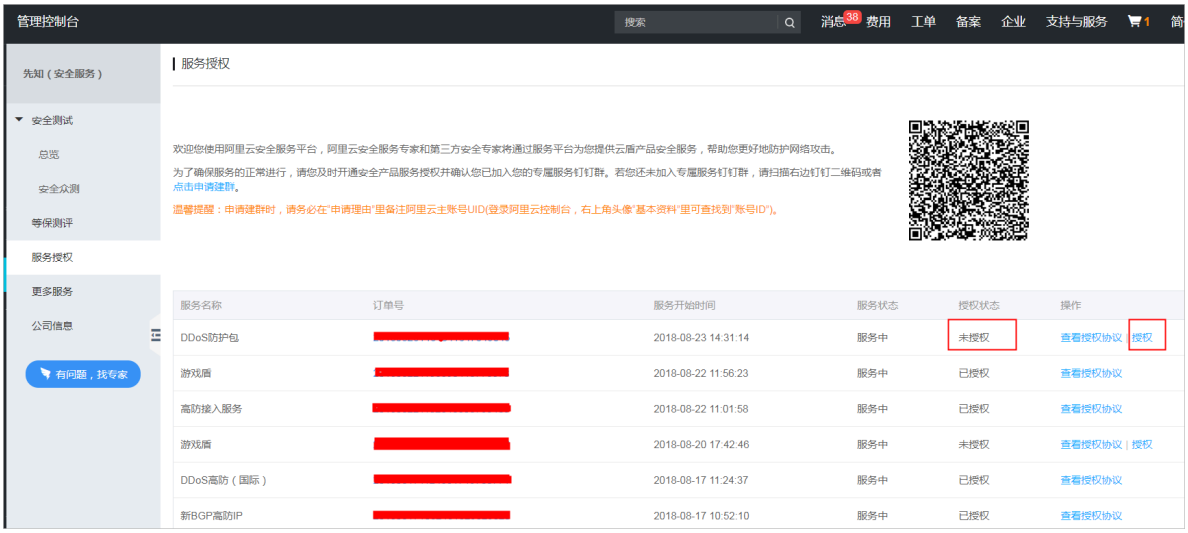
> **说明:**
> **您必须已购买或开通云盾高防产品，才能享受高防安全专家服务。**

操作步骤

1. **登录云盾先知（安全服务）管理控制台。**

2. 定位到服务授权页面，您可以查看到您的高防产品安全服务订单的授权情况。

> **说明:**
> 一般情况下，新创建的安全服务订单状态为未授权。



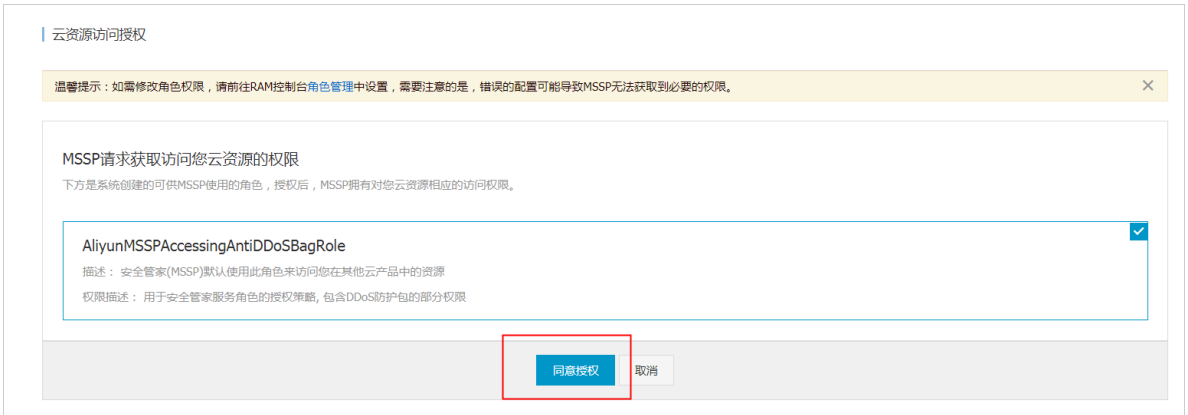
3. 单击查看授权协议，确认并同意授权书内容后，单击确定。

4. 单击授权。

5. 在服务订单所对应的云资源RAM角色授权页面，单击同意授权。

说明:

为了确保与安全专家的交流，确认您已申请并开通与安全专家的专属钉钉服务群。



预期结果

授权完成后，在云盾先知（安全服务）管理控制台的服务授权页面，该服务订单的状态显示为已授权，您可以随时单击查看授权协议查看授权书。

完成授权后，您的专属安全专家可以通过阿里云安全服务平台直接查看您的高防中相应的业务数据及配置数据，为您的业务提供专属的安全策略和建议。安全专家通过阿里云安全服务平台查看您高防控制台进行的所有操作都将产生相应的操作日志，您可以随时登录阿里云控制台查看安全专家操作记录。

4.7.2 查看安全专家操作日志

获得授权的安全专家可以通过阿里云安全服务平台访问并查看您高防控制台。安全专家在您的控制台上的所有操作都将产生操作日志。您可以随时登录阿里云操作审计管理控制台查看并审计这些操作行为。

操作步骤

1. **登录操作审计管理控制台，选择华东1（杭州）。**

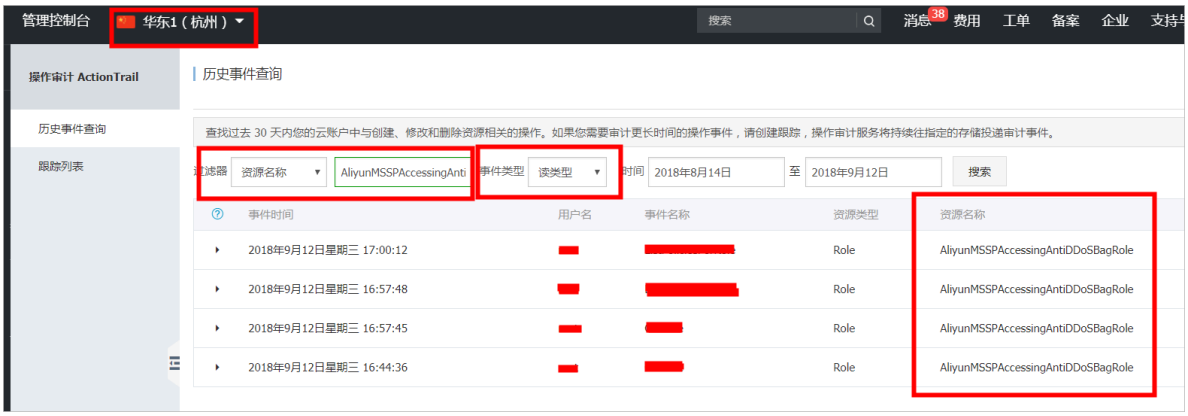
2. **定位到历史事件查询页面，设置以下查询条件，单击搜索，查询您的专属安全专家在高防控制台中的操作记录日志。**

- 资源名称：包含AliyunMSSPAccessingAntiDDoSBagRole
- 事件类型：所有类型

> **说明：**
> 目前高防安全服务仅授权安全专家查看您高防控制台中的数据，不具备更改配置等权限。因此，您也可以将事件类型条件设置为读类型，查询到的事件记录与选择所有事件类型得到的查询结果一致。

- 时间：选择您想查询的时间范围。

> **说明：**
> 历史事件查询支持查看最近30天内的操作记录。



3. 在事件列表中，单击操作记录可展开查看事件详情。

4. 单击查看事件可查看该事件的详细参数。

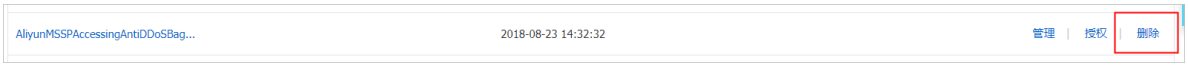
4.7.3 取消高防安全服务授权

高防安全服务授权开通后，您可以随时在访问控制（RAM）管理控制台中删除高防安全服务的授权角色，取消高防安全服务授权。

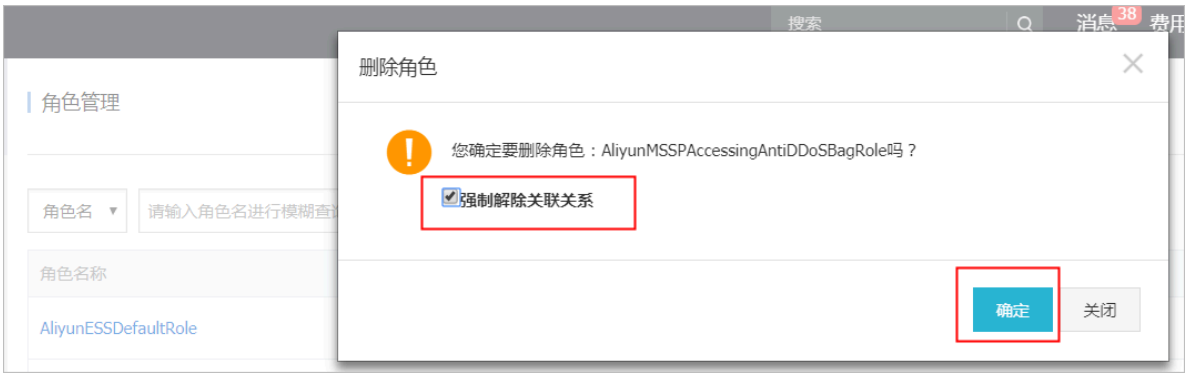
操作步骤

1. 登录访问控制（RAM）管理控制台。

2. 定位到角色管理页面，通过搜索角色名（包含“MSSP”）找到授权服务订单时生成的MSSP安全产品服务的授权角色。
   - 高防IP对应角色名称为：AliyunMSSPAccessingYundunHighRole
   - 高防（国际）对应角色名称为：AliyunMSSPAccessingDDoSDIPRole
   - 新BGP高防对应角色名称为：AliyunMSSPAccessingDDoSCOORole
   - 游戏盾对应角色名称为：AliyunMSSPAccessingGameShieldRole
   - DDoS防护包对应角色名称为：AliyunMSSPAccessingAntiDDoSBagRole
3. 单击相应角色后的删除。



4. 在删除角色对话框中勾选强制解除关联关系，并单击确定。



5. 获取并输入手机验证码，单击确定，通过手机验证。

预期结果

授权角色删除成功后，在云盾先知（安全服务）管理控制台的服务授权页面中相应服务订单的状态将变更为未授权。

4.8 安全专家指导服务

阿里云DDoS高防IP产品为您免费提供一对一的专家指导咨询服务。

背景信息

如果您在使用云盾DDoS高防IP产品过程中遇到任何问题，可以随时通过云盾DDoS高防IP管理控制台的专家咨询服务入口，申请加入高防产品专家咨询服务钉钉群。

届时，您在DDoS高防IP产品使用过程中遇到的任何问题，都将得到高防产品专家的妥善解决和处理。

操作步骤

1. 登录云盾DDoS防护管理控制台。
2. 将鼠标移至有问题？找专家！图标，使用钉钉扫描显示的二维码申请加入高防产品专家咨询群。

> **说明:**
> 您可以在云盾DDoS高防IP管理控制台的左侧导航栏、实例列表页面等位置找到专家咨询服务入口。

3. 成功加入高防产品专家咨询服务钉钉群后，安全专家将通过钉钉为您提供一对一指导服务，帮助您妥善解决DDoS高防IP产品使用过程中遇到的任何问题。

> **说明:**
> 您也可以选择通过电话联系我的方式，留下您的联系电话，安全专家收到您的申请后将会第一时间联系您。

5 最佳实践

5.1 DDoS高防接入配置最佳实践

将业务接入云盾DDoS高防产品，将攻击流量引流到DDoS高防，有效避免业务在遭受大流量DDoS攻击时出现服务不可用的情况，确保源站服务器的稳定可靠。

您可以参考本文中的接入配置和防护策略最佳实践，在各类场景中使用云盾DDoS高防更好地保护您的业务。

正常网站业务接入场景

业务梳理

首先，建议您对所需接入DDoS高防进行防护的业务情况进行全面梳理，帮助您了解当前业务状况和具体数据，为后续使用DDoS高防的防护功能模块提供指导依据。

梳理项	说明
网站和业务信息	
网站/应用业务每天的流量峰值情况，包括Mbps、QPS	判断风险时间点，并且作为DDoS高防实例的业务带宽和业务QPS规格的选择依据。
业务的主要用户群体（例如，访问用户的主要来源地区）	判断非法攻击来源。
源站服务器的操作系统（Linux、Windows）和所使用的Web服务中间件（Apache、Nginx、IIS等）	判断源站是否存在访问控制策略，避免源站误拦截DDoS高防回源IP转发的流量。
业务是否需要支持IPv6协议	DDoS高防暂未支持IPv6协议。如果您的业务需要支持IPv6协议，建议您使用*DDoS*防护包。
业务使用的协议类型	用于后续业务接入DDoS高防配置。
业务端口	判断源站业务端口是否在DDoS高防的支持端口范围内。 说明: 对于网站业务，DDoS高防目前仅支持80和443标准端口。
（针对HTTPS业务）服务端是否使用双向认证	DDoS高防暂不支持双向认证，需要变更认证方式。

梳理项	说明
（针对HTTPS业务）客户端是否支持SNI标准	对于支持HTTPS协议的域名，接入DDoS高防后，客户端和服务端都需要支持SNI标准。
（针对HTTPS业务）是否存在会话保持机制	如果业务部署了阿里云负载均衡（SLB）实例，建议开启Cookie会话保持功能。
业务是否存在空链接	例如，服务器主动发送数据包防止会话中断，这类情况下接入DDoS高防后可能会对正常业务造成影响。
业务交互过程	了解业务交互过程、业务处理逻辑，便于后续配置针对性防护策略。
活跃用户数量	便于后续在处理紧急攻击事件时，判断事件严重程度，以采取风险较低的应急处理措施。
业务及攻击情况	
业务类型及业务特征（例如，游戏、棋牌、网站、App等业务）	便于在后续攻防过程中分析攻击特征。
业务流量（入方向）	帮助后续判断是否包含恶意流量。例如，日均访问流量为100 Mbps，则超过100 Mpbs时可能遭受攻击。
业务流量（出方向）	帮助后续判断是否遭受攻击，并且作为是否需要额外业务带宽扩展的参考依据。
单用户、单IP的入方向流量范围和连接情况	帮助后续判断是否可针对单个IP制定限速策略。
用户群体属性	例如，个人用户、网吧用户、或通过代理访问的用户。判断是否存在单个出口IP集中并发访问导致误拦截的风险。
业务是否遭受过大流量攻击及攻击类型	根据历史遭受的攻击类型，设置针对性的DDoS防护策略。
业务遭受过最大的攻击流量峰值	根据攻击流量峰值判断DDoS高防功能规格的选择。
业务是否遭受过CC攻击（HTTP Flood）	通过分析历史攻击特征，配置预防性策略。
业务遭受过最大的CC攻击峰值QPS	通过分析历史攻击特征，配置预防性策略。
业务是否提供Web API服务	如果提供Web API服务，不建议使用CC攻击紧急防护模式。通过分析API访问特征配置自定义CC攻击防护策略，避免API正常请求被拦截。
业务是否已完成压力测试	评估源站服务器的请求处理性能，帮助后续判断是否因遭受攻击导致业务发生异常。

准备工作

：
在将业务接入DDoS高防时，强烈建议您先使用测试业务环境进行测试，测试通过后再正式接入生产业务环境。

在将业务接入DDoS高防前，您需要完成以下准备工作：

业务类型	准备工作
网站业务	· 所需接入的网站域名清单，包含网站的源站服务器IP（仅支持公网IP的防护）、端口信息等。 · 所接入的网站域名必须已完成阿里云备案。 · 如果您的网站支持HTTPS协议访问，您需要准备相应的证书和私钥信息，一般包含格式为 .crt 的公钥文件或格式为 .pem 的证书文件、格式为 .key 的私钥文件。 · 具有网站DNS域名解析管理员的账号，用于修改DNS解析记录将网站流量切换至DDoS高防。 · 推荐在将网站业务接入前，完成压力测试。 · 检查网站业务是否已有信任的访问客户端（例如监控系统、通过内部固定IP或IP段调用的API接口、固定的程序客户端请求等）。在将业务接入后，需要将这些信任的客户端IP加入白名单。
非网站业务	· 对外提供服务的端口、协议类型。 · 如果业务通过域名访问，需要准备DNS域名解析管理员账号，用于修改DNS解析记录将网站流量切换至DDoS高防。 · 推荐在将业务接入前，完成压力测试。

DDoS高防配置

1. 业务接入配置

   根据您的业务场景和所选购的DDoS高防产品，参考以下接入配置指导，将您业务接入DDoS高防：

   · 网站类业务接入*DDoS*高防*IP*
   · 非网站类业务接入*DDoS*高防*IP*

- 业务接入DDoS新BGP高防
- 通过NS方式将网站类业务接入DDoS新BGP高防
- 网站类业务接入DDoS高防（国际）（适用于部署在非中国大陆地区的业务）
- 非网站类业务接入DDoS高防（国际）（适用于部署在非中国大陆地区的业务）

> 说明:
> - 将非网站类业务接入DDoS高防前，务必确认业务的服务类型。如果存在服务端主动发送数据包的场景，需要关闭空链接防护策略，避免正常业务受到影响。
> - 对于网站类业务，由于CC安全防护的攻击紧急模式可能会对特定类型的业务造成一定的误拦截，不建议将攻击紧急作为CC安全防护的默认防护模式。

2. 源站保护配置

为避免恶意攻击者绕过DDoS高防直接攻击源站服务器，建议您完成源站保护配置。

3. 防护策略配置

a. 网站域名类业务（仅支持80、443标准端口）

- CC攻击防护
  - 业务正常时：将网站业务接入DDoS高防后，建议您在运行一段时间后（两、三天左右），通过分析业务应用日志数据（包括URL、单一源IP平均访问QPS等），评估正常情况下单访问源IP的请求QPS情况并相应配置CC防护自定义规则限速策略，避免遭受攻击后的被动响应。
  - 正在遭受CC攻击时：通过查看管理控制台的概览报表，获取域名请求TOP URL、IP地址、访问来源IP、User-agent等参数信息，根据实际情况制定CC防护自定义规则，并观察防护效果。

    > 说明:
    > 如果实际防护效果不佳，您可以联系阿里云安全服务专家，协助您进一步分析日志并制定防护策略。

    > :
    > 由于CC安全防护的攻击紧急模式可能会对特定类型的业务造成一定的误拦截，如果您的业务类型为App业务或者Web API服务，建议您不要使用攻击紧急CC安全防护模式。
- 开启全量日志

强烈建议您开启全量日志服务。当业务遭受网络七层攻击时，可以通过全量日志功能分析攻击行为特征，针对性制定防护策略。

说明:

- 开通全量日志服务将可能产生额外费用，请您在开通服务前确认。
- 当已存储的日志容量达到3 TB，将停止存储新生成的网站日志。您拥有三次机会清空当前存储的所有日志数据，或者您可以通过关闭一些不必要的网站的日志存储功能来减少日志存储量。
- 免费日志存储规格默认保存最近30天的日志。当存储的日志数据超过30天后，将自动被新的日志数据覆盖。

b. 非网站端口类业务

一般情况下，将非网站业务接入DDoS高防后，采用默认防护配置即可。在运行一段时间后（两、三天左右），您可以根据业务情况调整清洗模式（DDoS高防IP）或智能防御模式（新BGP高防），可有效提升针对网络四层CC攻击的防护效果。

如果您发现有攻击流量透传到源站服务器的情况，建议您启用DDoS防护策略中的源、目的连接限速策略。在不完全清楚业务情况时，建议将新建连接限速和并发连接限速均设置为5。如果发现存在误拦截的现象，您可调整数值，适当放宽限速策略。

:

如果存在服务端主动发送数据包的业务场景，需要关闭空链接防护策略，避免正常业务受到影响。

说明:

如果在接入DDoS高防前业务已遭受攻击，建议您更换源站服务器IP。更换IP前，请务必确认是否在客户端或App端中通过代码直接指向源站IP，在这种情况下，请先更新客户端或App端代码后再更换源站IP，避免影响业务正常访问。

4. 本地测试

完成上述DDoS高防配置后，建议您进行配置准确性检查和验证测试。

说明:

您可以通过修改本地系统Hosts文件方式进行本地测试。

表 5-1: 配置准确性检查项

编号	检查项
网站域名类业务接入检查项	
1	接入配置域名是否填写正确（必检项）
2	域名是否备案（必检项）
3	接入配置协议是否与实际协议一致（必检项）
4	接入配置端口是否与实际提供的服务端口一致（必检项）
5	源站填写的IP是否是真实服务器IP，而不是错误地填写了高防IP或其他服务IP（必检项）
6	证书信息是否正确上传（必检项）
7	证书是否合法（例如，加密算法不合规、错误上传其他域名的证书等）（必检项）
8	证书链是否完整（必检项）
9	是否已了解DDoS高防实例的弹性防护计费方式（必检项）
10	协议类型是否启用Websocket、Websockets协议（必检项）
非网站端口类业务检查项	
1	业务端口是否可以正常访问（必检项）
2	接入配置协议是否与实际协议一致；确认未错误地为TCP协议业务配置UDP协议规则等（必检项）
3	源站填写的IP是否是真实服务器IP，而不是错误地填写了高防IP或其他服务IP（必检项）
4	是否已了解DDoS高防实例的弹性防护计费方式（必检项）

表 5-2: 业务可用性验证项

编号	检查项
1	测试业务是否能够正常访问（必检项）
2	测试业务登录会话保持功能是否正常（必检项）
3	（网站域名类业务）观察业务返回4XX和5XX响应码的次数，确保回源IP未被拦截（必检项）
4	（网站域名类业务）对于App业务，测试HTTPS链路访问是否正常；检查是否存在SNI问题（必检项）
5	是否配置后端真实服务器获取真实源IP（建议项）

编号	检查项
6	（网站域名类业务）是否配置源站保护，防止攻击者绕过DDoS高防直接攻击源站（建议项）
7	测试TCP业务的端口是否可以正常访问（必检项）

5. 正式切换业务流量

必要测试项均通过后，修改DNS解析记录，将网站业务流量切换至DDoS高防。

> 说明:
> 修改DNS解析记录后，需要10分钟左右生效。

真实业务流量切换后，您需要再次根据上述业务可用性验证项进行测试，确保业务正常运行。

6. 监控告警配置

建议您使用云监控功能对已接入DDoS高防进行防护的域名、端口和业务源站端口进行监控，实时监控其可用性、HTTP返回状态码（5XX、4XX类状态码）等，及时发现业务异常现象。

7. 日常运维

- 弹性后付费和保险版高级防护次数
  - 首次购买新BGP高防的用户可以免费获得三个300 G规格的抗D包，建议您尽快将其绑定至DDoS高防实例并将弹性防护阈值设置为300 G。绑定成功后，当日内（自然日）所遭受的抗D包防护规格内（300 G以内）的攻击防护流量将不会产生弹性防护费用。

    > 说明:
    > 如果您在抗D包耗尽后或到期后不想启用DDoS高防的弹性防护能力，应及时将弹性防护阈值调整为实例的保底防护带宽。

  - 如果需要启用DDoS高防的弹性防护能力，请务必先查看DDoS高防的计费方式，避免出现实际产生的弹性防护费用超出预算的情况。
  - DDoS高防（国际）的保险版实例，每月免费赠送两次高级防护（无上限全力防护）。建议您根据业务需求情况选择对应的套餐版本。
- 判断攻击类型

  当DDoS高防同时遭受CC攻击和DDoS攻击时，您可在云盾DDoS防护管理控制台的安全报表中，根据攻击流量信息判断遭受的攻击类型。

  - DDoS攻击类型：在DDoS攻击防护报表中有攻击流量的波动，且已触发流量清洗，但在CC攻击防护报表中不存在相关联的波动。

- CC攻击类型： 在DDoS攻击防护报表中有攻击流量的波动，已触发流量清洗，且在CC攻击防护报表中有相关联的波动。

· 业务访问延时或丢包

- 针对源站服务器在海外、DDoS高防实例为中国大陆地区、主要访问用户来自中国大陆地区的情况，如果用户访问网站时存在延时高、丢包等现象，可能是由于回源网络链路问题，推荐您将源站服务器部署在中国大陆地区。
- 针对源站服务器在海外、DDoS高防实例为海外地区、主要访问用户来自中国大陆地区的情况，如果用户访问网站时存在延时高、丢包等现象，可能存在跨网络运营商导致的访问链路不稳定，推荐您使用DDoS高防（国际）实例并搭配加速线路。

· 删除域名或端口转发配置

如果需要删除已防护的域名端口转发配置记录，确认业务是否已正式接入DDoS高防。

- 如果尚未正式切换业务流量，直接在云盾DDoS防护管理控制台中删除域名或端口转发配置记录即可。
- 如果已完成业务流量切换，删除域名或端口转发配置前务必前往域名DNS解析服务控制台，修改域名解析记录将业务流量切换回源站服务器。

说明:

- 删除转发配置前，请务必确认域名的DNS解析或业务访问已经切换至源站服务器。
- 删除域名配置后，DDoS高防将无法再为您的业务提供专业级安全防护。

业务遭受攻击时的紧急接入场景

如果您的业务已经遭受攻击，建议您在将业务接入DDoS高防前执行以下操作：

· 遭受DDoS攻击

一般情况下，将业务接入DDoS高防后，采用默认防护配置即可。

如果您发现有网络四层CC攻击透传到源站服务器的情况，建议您启用DDoS防护策略中的源、目的连接限速策略。

· 源站IP已被黑洞

如果接入DDoS高防前，业务源站服务器已被攻击且触发黑洞策略，应及时更换源站*ECS IP*（如果源站为SLB实例，则更换SLB实例公网IP）。更换源站IP后，请尽快将业务接入DDoS高防进行防护，避免源站IP暴露。

如果您不希望更换源站IP，或者已经更换源站IP但仍存在IP暴露的情况，建议您在源站ECS服务器前部署负载均衡（SLB）实例，并将SLB实例的公网IP作为源站IP接入DDoS高防。

> 说明:
> 如果您的业务源站服务器未部署在阿里云，遭受攻击后需要紧急接入DDoS高防进行防护，请确认您业务使用的域名已通过工信部备案，并在将业务接入DDoS高防前联系阿里云技术支持人员对域名进行特殊处理，避免由于域名未通过阿里云备案，导致业务无法正常访问。

- 遭受CC攻击或爬虫攻击

  业务遭受CC攻击、爬虫攻击，在将业务接入DDoS高防后，需要通过分析HTTP访问日志，判断攻击特征并设置相应的防护策略（例如，分析访问源IP、URL、Referer、User Agent、Params、Header等请求字段是否合法）。如果仍然存在攻击流量透传至源站的情况，请联系阿里云技术支持人员。

安全专家服务

购买开通云盾DDoS高防后，您可以在管理控制台中通过钉钉扫描二维码直接联系阿里云安全服务专家。

安全专家将针对您的业务场景提供DDoS高防接入配置指导、安全攻击分析和防御相关安全服务，基于业务实际情况帮助您更好地使用DDoS高防对业务进行安全防护，保障您业务的网络安全。

说明:

为了便于快速分析和解决问题，在远程技术支持服务过程中，可能需要您授权阿里云安全专家查看业务数据。所有安全专家服务人员都将严格遵循服务授权和保密原则，防止您的信息泄露。

5.2 设置DDoS高防IP的自定义告警规则

该章节介绍如何在云监控控制台上设置DDoS高防IP的自定义告警规则。通过自定义告警规则功能，您能够使告警服务更加符合自身的业务需求。

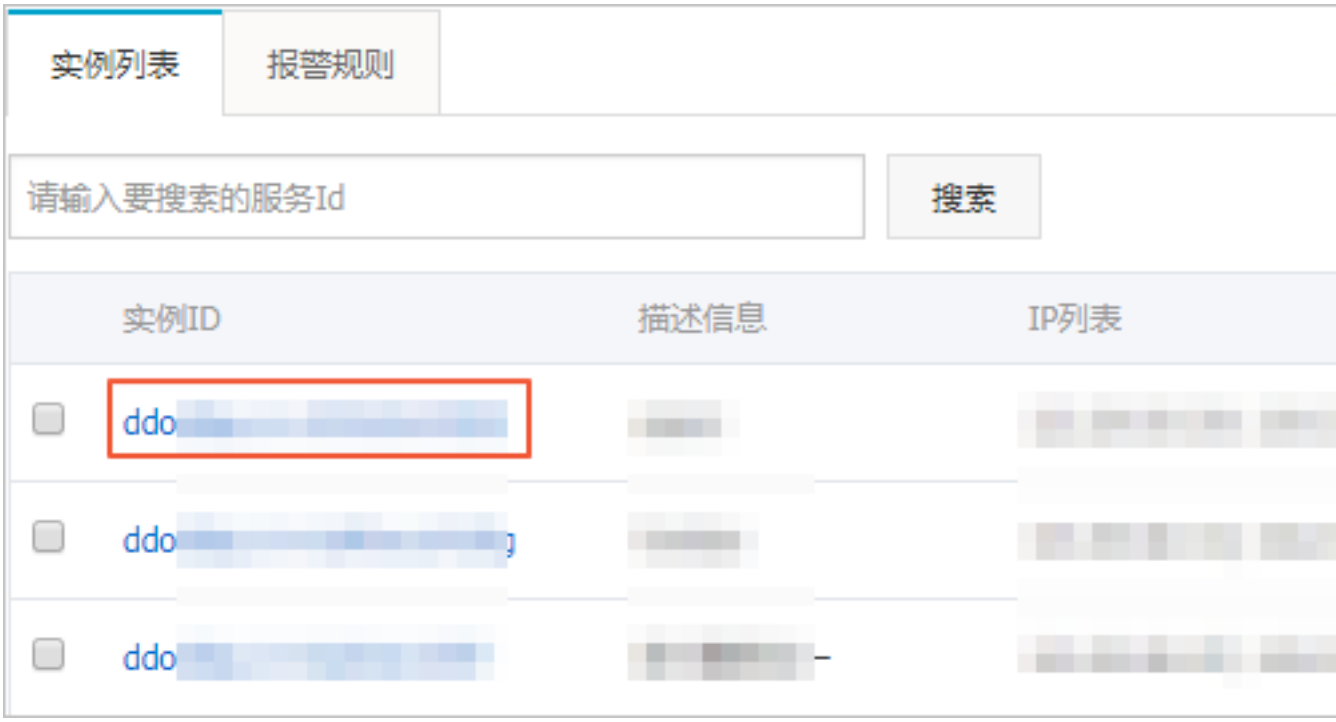
背景信息

自定义告警规则参数说明如下：

参数	说明
监控项	即DDoS高防IP服务提供的监控指标。
统计周期	报警系统会按照这个周期检查您对应的监控数据是否超过了报警阈值。 例如设置高防IP入流量报警规则的统计周期为1分钟，则每间隔1分钟会检查一次高防IP入流量是否超过了阈值。
连续次数	指连续几个统计周期监控项的值持续超过阈值后触发报警。

操作步骤

1. 登录云监控控制台，定位到云服务监控 > DDoS高防IP。
2. 在实例列表中，单击高防实例名称或操作栏中的监控图表，即可进入DDoS高防IP的实例监控图表页面。



3. 单击监控图右上角的铃铛按钮或页面右上角的新建报警规则，可对该实例对应的监控项设置报警规则。

   具体报警服务规则设置指导可以参考云监控报警服务帮助文档。

5.3 查看DDoS高防IP的实时监控数据

该章节介绍如何在云服务控制台上查看DDoS高防IP的实时监控数据。通过查看DDoS高防IP的实时监控数据，帮助您全面了解业务的DDoS高防IP的防护情况。

背景信息

DDoS高防IP的实时监控数据包括以下：

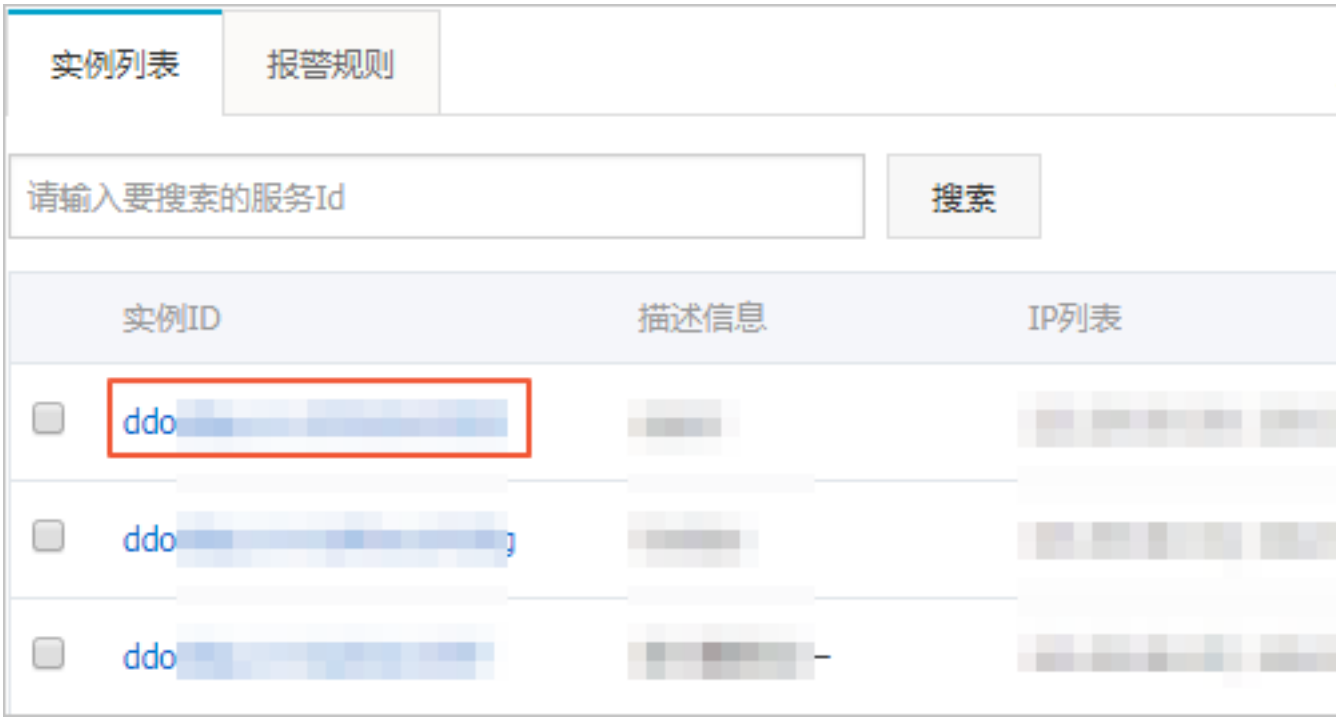
监控项	维度	单位
高防IP出流量	实例维度、IP维度	bit/s
高防IP入流量	实例维度、IP维度	bit/s
高防IP回源带宽	实例维度、IP维度	bit/s
高防IP攻击流量	实例维度、IP维度	bit/s
高防IP活跃并发连接	实例维度、IP维度	个
高防IP非活跃并发连接	实例维度、IP维度	个
高防IP新建连接	实例维度、IP维度	个

说明:

高防IP回源带宽是指通过高防清洗后回源到源站服务器的干净业务流量带宽。

操作步骤

1. 登录云监控控制台，定位到云服务监控 > DDoS高防IP。
2. 在实例列表中，单击高防实例名称或操作栏中的监控图表，即可进入DDoS高防IP的实例监控图表页面。



3. 单击页面上方的时间范围快速选择按钮或精确选择时间段，查看各项监控项数据。

   监控数据最长支持查看连续30天的监控数据。

4. 单击监控图右上角的放大按钮，可查看监控大图。

5.4 多线路高防实例回源到不同源站的配置方法

出于合规或者高可用的需求，您可能需要将一个多线路高防IP实例配置回源到不同的源站。例如，将高防实例的电信线路回源到您的电信源站，联通线路回源到联通源站。本文介绍了相关配置方法。

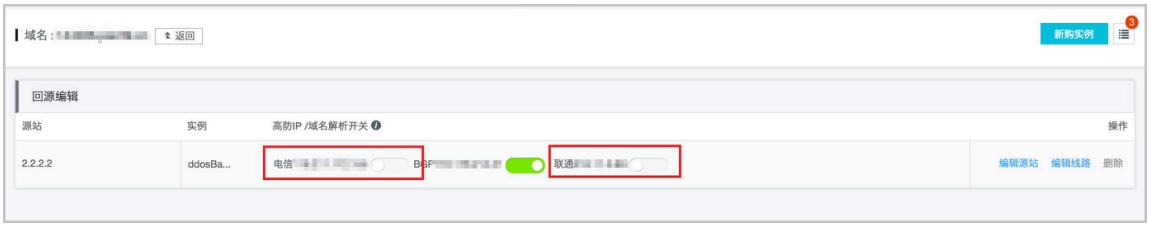
背景信息

如果您还未将需要配置的域名接入高防 IP 实例，请参考*HTTP*网站接入或*HTTPS*网站接入将您的域名添加至已购买的高防 IP 实例。

> **说明:**
> 建议您先使用测试域名熟悉配置步骤后，再进行实际操作配置。建议您在业务低峰期进行操作。

操作步骤

1. 登录云盾DDoS防护管理控制台，并前往接入 > 网站。
2. 选择您需要进行配置的域名，并单击其域名信息下的回源编辑。
3. 修改该域名的回源配置，关闭部分线路。
   a) 单击高防IP/域名解析开关下的启停开关，关闭部分线路的域名解析。例如，假如您想要将当前配置的源站作为 BGP 线路的回源源站，您可以关闭电信线路及联通线路的解析。



   b) 单击 操作列下的编辑线路。
   c) 在编辑线路页面，单击已关闭域名解析的线路下的停用，停用线路。例如，停用电信线路及联通线路。

   d) 单击确定，回到回源编辑页面。可以看到，部分线路已经关闭。

4. 添加转发规则，配置其它线路的回源源站。
   a) 单击添加转发规则，添加其它线路的源站 IP。例如，添加电信线路的回源源站 IP。

b) 选择启用高防 IP 实例的电信线路，单击确定。

c) 添加完成后，高防实例的电信线路会回源到配置的电信线路源站。

5. 参考步骤4，将该高防 IP 实例的其它线路配置到相应线路的源站，使不同的网络运营商线路回源到不同源站。

5.5 云外主机获取真实客户端源IP

如果您为阿里云外主机配置了 DDoS 高防 IP 服务，您可以使用本文介绍的方法来获取真实客户端源 IP。

本文介绍的方法支持以下操作系统：

- Redhat Linux
- Centos 6.x

在按照步骤进行操作前，请注意以下事项：

- 建议先在测试环境中进行测试，观察环境稳定后再部署正式上线。
- 建议保留原有的内核，如果出现重启失败，可以切换到原有内核进行恢复。

操作步骤

参照以下步骤，来获取真实客户端源IP。

1. 下载内核安装文件。
   - *kernel-2.6.32-220.23.2.ali_github.el6.x86_64.rpm*
   - *kernel-firmware-2.6.32-220.23.2.ali_github.el6.x86_64.rpm*
2. 安装内核。定位到安装文件目录，执行以下命令：

```
rpm -ivh kernel-2.6.32-220.23.2.ali_github.el6.x86_64.rpm
```

说明:

CentOS 6.2 以上版本不需要安装 kernel-firmware。

3. 设置 toa 模块启动自动加载。
   a. 创建文件*/etc/sysconfig/modules/toa.modules*，文件内容如下：

```
!/bin/bash
if [ -e /lib/modules/uname -r/kernel/net/toa/toa.ko ] ;
then
modprobe toa > /dev/null 2>&1
fi
```

   b. 执行以下命令，授予创建 toa 模块可执行权限：

```
sudo chmod +x /etc/sysconfig/modules/toa.modules
```

4. 执行`reboot`命令，重启系统。

功能测试

安装完成后，主机应能正常获取真实客户端源 IP。如果仍无法获取客户端源 IP，可执行`lsmod | grep toa`命令检测 toa 模块加载情况。

如果 toa 模块未加载，通过执行`modprobe toa`命令手动加载。加载成功后，重新测试主机能否获取真实客户端源 IP。

相关问题

- 网络连接通过 toa 模块转换，对性能有多大影响?

  toa 模块是部署在旁路的，因此对网络性能几乎没有影响。

- 如果担心加载新的内核模块可能出现稳定性问题怎么办?

  建议保留原有的内核，如果出现重启失败，可以切换到原有内核恢复。另外，当前版本是在Github上开源的。

5.6 “高防IP+阿里云CDN”同时接入

不建议使用DDoS高防IP后再回源至阿里云CDN，可能存在无法访问，网站异常等情况。

目前已经提供SCDN方案，为网站做加速的同时，防护DDoS，CC等DDoS攻击行为。

具体产品详情及介绍：https://www.aliyun.com/product/scdn

5.7 "高防IP+云盾WAF"同时使用

DDoS高防IP完全兼容云盾Web应用防火墙。本文介绍了同时接入高防IP、Web应用防火墙的方法。

背景信息

在同时接入高防IP、Web应用防火墙 最佳的部署架构如下：

高防IP（入口层，DDoS防护）> Web应用防火墙（中间层，应用层防护） > 源站（ECS/SLB/VPC/IDC...）

说明:

经过WAF多层转发后，HTTP头部的X-Forwarded-For字段包含请求用户的真实IP，和所有经过的中间代理服务器的IP。其中，用户的真实IP处在第一个位置。例如，

```
X-Forwarded-For：用户真实IP，代理服务器1-IP，代理服务器2-IP，代理服务器3-IP，…
```

因此，要获取用户的真实IP，需要获取HTTP头部的X-Forwarded-For字段内容。具体方法，请参考如何获取客户端真实IP。

参照以下步骤，同时接入高防IP、Web应用防火墙。

操作步骤

1. 配置Web应用防火墙。在源站IP中填写SLB公网IP、ECS公网IP或本地服务器IP，并在是否已使用了高防、CDN、云加速等代理？选项下选择是。

Web应用防火墙配置完成后，会生成一个CNAME。

2. 配置DDoS高防IP。在源站域名中填入Web应用防火墙提供的CNAME。

3. 在DNS解析处，修改DNS配置，将域名解析指向高防IP服务生成的CNAME。这样，流量会先经过高防IP，再转发至Web应用防火墙。

5.8 如何通过高防IP判断遭受的攻击类型

当高防 IP 同时遭受 CC 攻击和 DDoS 攻击时，您可参考以下方法快速判断遭受的攻击类型，并进行对应的处理。

- CC 攻击：主要作用于七层网站连接数的攻击。
- DDoS 攻击：主要作用于四层流量的攻击。

快速判断方法

根据您的配置情况，您可在云盾*DDoS*防护管理控制台的统计 > 安全报表中，根据攻击流量信息判断遭受的攻击类型。

- DDoS 攻击类型：在DDoS攻击防护报表中有攻击流量的波动，且已触发流量清洗，但在CC攻击防护报表中不存在相关联的波动。
- CC 攻击类型：在DDoS攻击防护报表中有攻击流量的波动，已触发流量清洗，且在CC攻击防护报表中有相关联的波动。

由于DDoS攻击防护报表记录的是四层相关的流量信息，而CC攻击是针对七层的攻击，需要在CC攻击防护报表中才能看到相关的防护结果。

5.9 如何将已配置高防的业务切换至其他高防实例

原高防 IP 实例已经到期，重新购买了新的高防 IP 实例，需要在业务不中断的前提下进行业务迁移。

操作步骤

1. 登录 云盾*DDoS*防护管理控制台。
2. 定位到接入 > 网站页面。
3. 选择您需要切换高防 IP 实例的域名，单击其域名信息下的回源编辑。
4. 单击操作列下的编辑线路。
5. 在编辑线路对话框中，选择您想要使用的新的高防 IP 实例中的线路，单击启用将配置下发到新高防 IP 实例中的线路。
6. 单击确定。待配置生效后，该域名配置已同时下发至原高防 IP 实例和新高防 IP 实例。
7. 在回源编辑页面关闭原高防 IP 实例线路的域名解析，然后在编辑线路对话框中停用原高防 IP 实例线路，完成高防 IP 实例切换。

5.10 源站IP暴露的解决办法

在配置 DDoS 高防 IP 服务后，如果还存在攻击绕过高防直接攻击源站 IP 的情况，需要更换源站 IP。

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。

排查步骤

为确保没有其他可能暴露源站 IP 的因素，建议您按照下列步骤进行逐一排查：

1. 源站服务器中是否存在木马、后门之类的安全隐患。

   如果没有相应的安全技术人员进行排查，可以选择云盾 安全管家、安骑士服务，或者前往云市场选择相关的安全服务。

2. 源站 IP 是否存在一些其他的服务没有配置高防 IP 服务，如邮件服务器的 MX 记录、bbs记录等除 Web 以外的记录。

   说明:

   请仔细检查您 DNS 解析的全部内容，确保没有记录解析到源站IP。

3. 是否存在网站源码信息泄露，如 `phpinfo()` 指令中可能包含的IP地址等泄露。
4. 是否存在某些恶意扫描情况。您可通过在源站上只允许高防回源 IP 来防护，详情请参考高防源站保护。
5. 确认已经没有业务解析到源站。

   a. 通过17测等工具测试当前的域名，查看是否还有解析到源站的情况。

   b. 再次检查您的 DNS 解析配置，查看是否还存在解析到源站 IP 的记录。

更换源站 IP

确认没有其他可能暴露源站 IP 的因素之后，更换已暴露的源站 IP。具体操作请参考更换*ECS IP*。

不想更换源站 IP 或已经更换过 IP

如您不想更换源站 IP 或者已经更换过源站 IP 但仍存在 IP 暴露情况，强烈建议您在后端ECS服务器前再部署一台负载均衡(SLB)服务器。

您可以使用以下部署架构：客户端 > 高防 IP > SLB > ECS

说明:

在此部署架构情况下，需要在高防 IP 管理控制台中填写负载均衡服务器的 IP 作为回源地址。

采用这种部署架构，即使攻击直接攻击源站，使得源站 IP 被黑洞，通过高防 IP 访问服务器依然不受影响。因为负载均衡服务器到源站的访问流量通过内网传输，即使源站 IP 被黑洞，高防 IP 仍然可以通过负载均衡服务器访问源站。

5.11 获取客户端真实IP

为Web业务部署DDoS防护后，您可以参照本文介绍的方法，获取客户端真实IP。

四层接入（非网站防护）

按照以下不同的部署配置场景，选择适合您的源站获取客户端IP方式。

- 高防 > 阿里云ECS

  通过TCP端口转发流量的情况，您无需做任何改动。源站服务器上看到的客户端IP就是真实的客户端IP。同时，ECS的安全组配置对象也可以针对真实的客户端IP进行设置。

  > 说明:
  > 如使用UDP端口转发，源站ECS将无法获取真实客户端IP。

- 高防 > SLB > ECS

  默认支持获取客户端真实IP。

  通过TCP端口转发流量的情况，您无需做任何改动。源站服务器上看到的客户端IP就是真实的客户端IP。

  > 说明:
  > - 负载均衡SLB访问控制设置白名单中必须添加高防回源IP段。
  > - 如使用UDP端口转发，源站ECS将无法获取真实客户端IP。

  > 注意:
  > - 2018年10月后创建的ECS实例，默认支持获取客户端真实IP，即在源站ECS服务器上看到的客户端IP就是真实访问源IP。
  > - 2018年10月前创建的ECS实例，默认情况下无法获取客户端真实IP，您需提交工单申请开通相关配置。

- 高防 > 阿里云外服务器

  部分情况下支持获取客户端真实IP，具体方法参考高防如何支持云外主机获取客户端IP。

七层接入（网站防护）

当一个七层代理服务器（如高防IP）把用户的访问请求转到后端服务器时，源站默认看到的是这个七层代理服务器（如高防IP）的回源IP。而真实的客户端IP会被七层代理服务器放在HTTP头部的X-Forwareded-For字段，格式如下：`X-Forwarded-For：用户真实IP，高防代理IP`。

如果中间经过不止一个代理服务器（如经过了WAF、CDN等等代理服务器），此时HTTP头部的X-Forwarded-For字段的格式如下：`X-Forwarded-For：用户真实IP，代理服务器1-IP，代理服务器2-IP，代理服务器3-IP，…`。

经过多层代理服务器，请求用户的真实IP处于第一个位置，而后面包含所有经过的中间代理服务器的IP。因此，只要获取HTTP头部的X-Forwarded-For字段的内容即可。

常用的获取X-Forwarded-For字段内容方式

- 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”)
```

获取到HTTP头部的X-Forwarded-For字段的相关内容后，以“,”作为区分符，截取其中的第一个IP地址即可获取客户端真实IP。

附录：常见Web服务器获取真实IP的方法

Nginx配置方案

1. 确认 http_realip_module 模块已安装。Nginx作为负载均衡获取真实IP是使用http_realip_module模块。

> 说明:
> 通过一键安装包安装的Nginx默认不安装此模块，可以使用 `# nginx -V | grep http_realip_module` 查看此模块有无安装。

如果 http_realip_module 模块未安装，需要重新编译Nginx并加装此模块。

```
wget http://soft.phpwind.me/top/nginx-1.0.12.tar.gz
```

```
tar zxvf nginx-1.0.12.tar.gz
cd nginx-1.0.12
./configure --user=www --group=www --prefix=/alidata/server/nginx --
with-http_stub_status_module --without-http-cache --with-http_ssl_m
odule --with-http_realip_module
make
make install
kill -USR2 `cat /alidata/server/nginx/logs/nginx.pid`
kill -QUIT `cat /alidata/server/nginx/logs/ nginx.pid.oldbin`
```

2. 修改Nginx对应server的配置。 在`location / {}`中添加以下内容。

```
set_real_ip_from ip_range1;
set_real_ip_from ip_range2;
...
set_real_ip_from ip_rangex;
real_ip_header    X-Forwarded-For;
```

说明:

这里的`ip_range1,2,...`指的是高防IP的回源IP地址，需要添加多条。如果高防IP后还有WAF、CDN，则需要写WAF、CDN的回源IP地址，即需要写离源站最近的一层七层代理的回源IP段。

3. 修改日志记录格式 log_format。log_format一般在nginx.conf中的HTTP配置中：

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

添加x-forwarded-for字段，替换原本的remote-address。

```
http {
    include       /etc/nginx/mime.types;
    default_type  application/octet-stream;

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

    access_log  /var/log/nginx/access.log  main;

    sendfile        on;
    #tcp_nopush     on;
```

4. 重启Nginx使配置生效`nginx -s reload`。

IIS 6 配置方案

IIS 6通过日志可获取来访者真实IP。

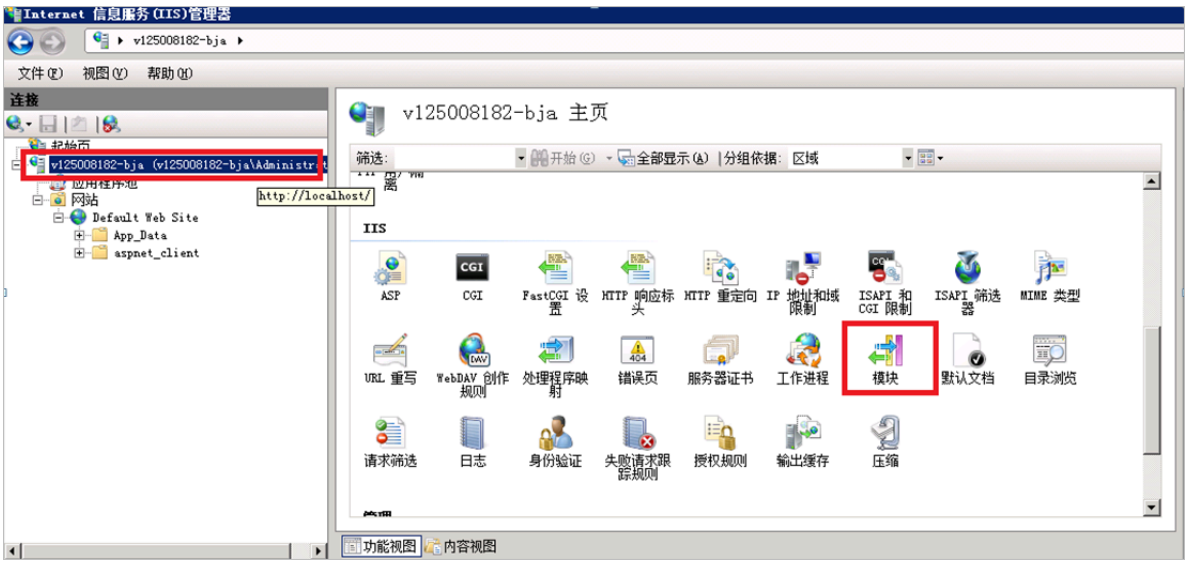
1. 安装*F5XForwardedFor.dll* 插件。
2. 根据您服务器的操作系统版本将*x86\Release*或者*x64\Release*目录下的*F5XForwardedFor.dll*拷贝到本地目录（例如*C:\ISAPIFilters*）。同时，确保IIS进程对该目录有读取权限。
3. 打开IIS管理器，选择当前开启的网站右键，单击属性。
4. 在属性对话框，单击ISAPI筛选器，单击添加。

5. 在添加对话框中，在筛选器名称处填写“F5XForwardedFor”，在可执行文件处填写F5XForwardedFor.dll的完整路径，单击确定。
6. 重启IIS服务器，配置生效。

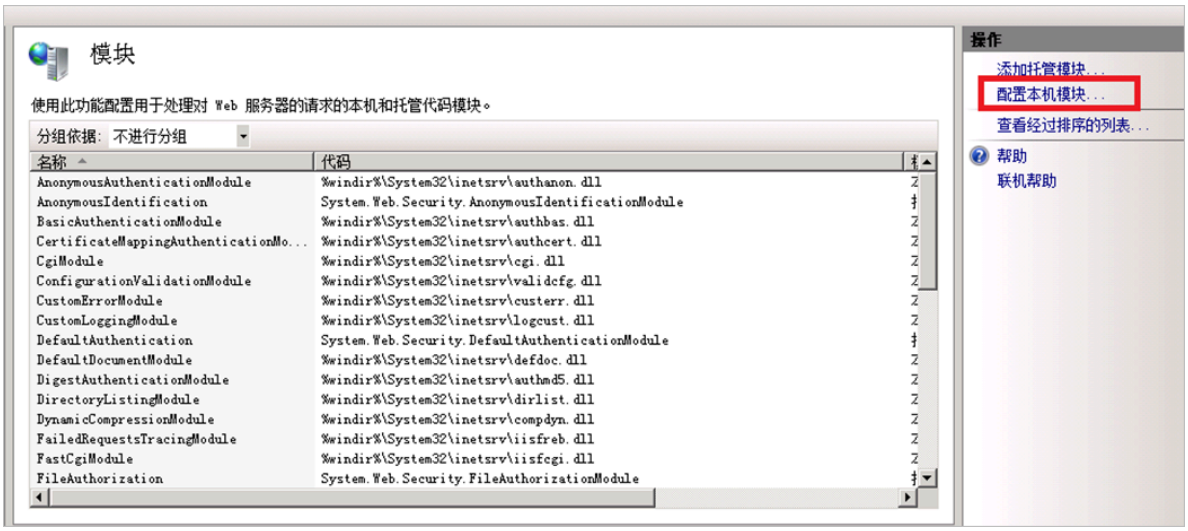
IIS 7 配置方案

IIS 7可通过F5XForwardedFor模块获取来访者真实IP。

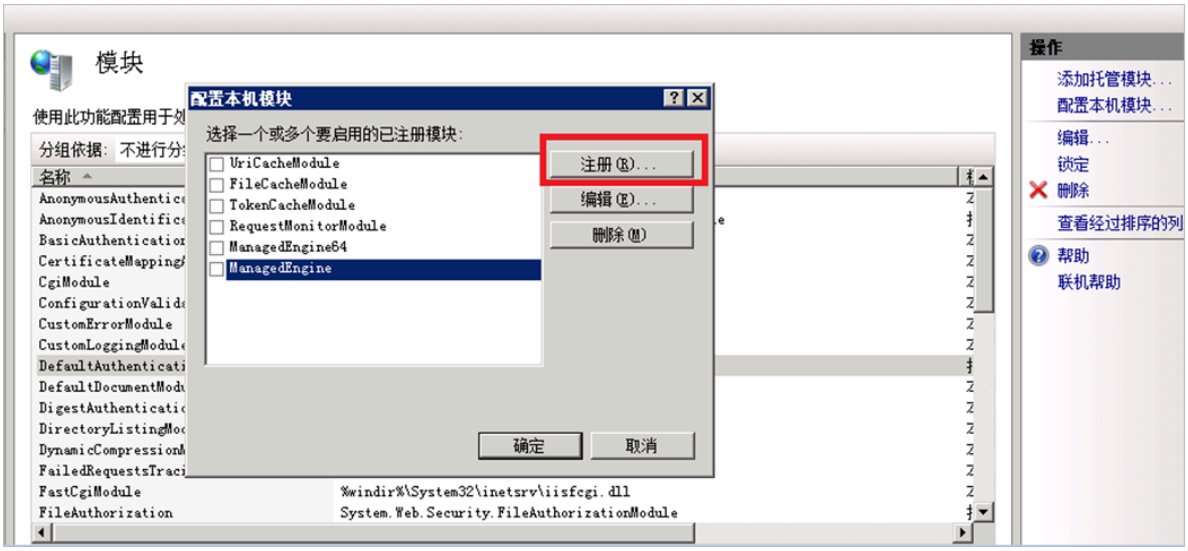
1. 下载并安装 *F5XForwardedFor* 插件模块。
2. 根据您服务器的操作系统版本将`x86\Release` 或者`x64\Release`目录下的`F5XFFHttpModule.dll` 和 `F5XFFHttpModule.ini` 文件拷贝到本地目录（例如 `C:\F5XForwardedFor\`）。同时，确保对IIS进程对该目录有读取权限。
3. 打开IIS管理器，选择IIS服务器选项。



4. 双击打开模块功能，单击配置本机模块。

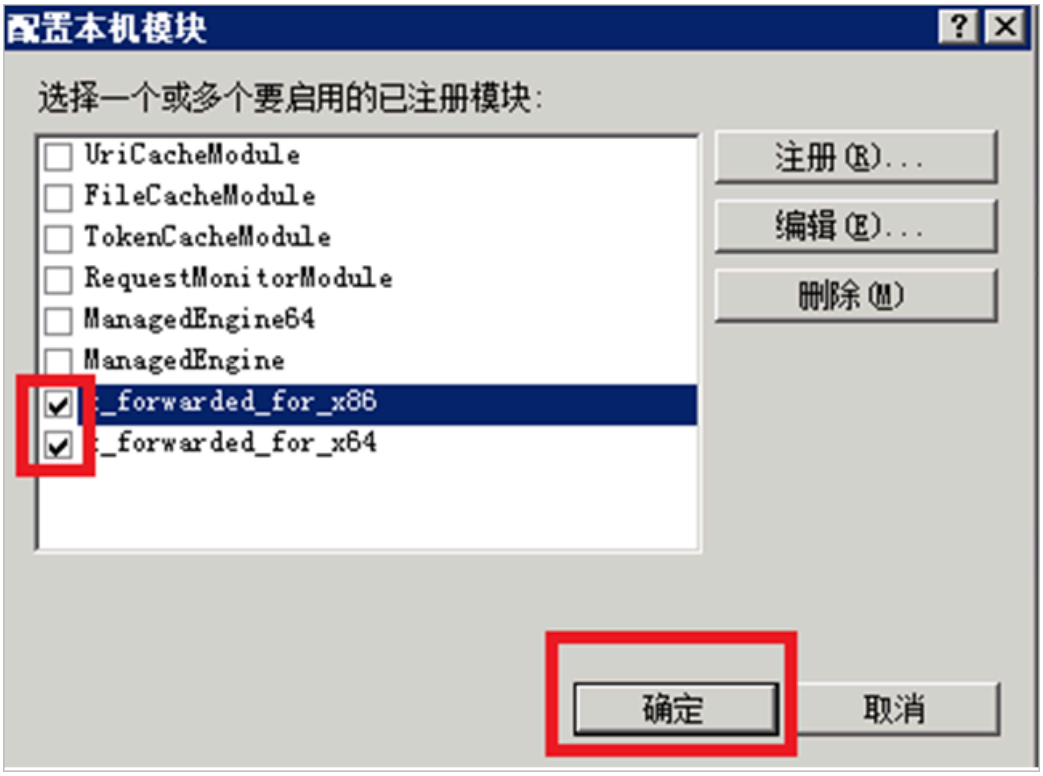


5. 在配置本机模块对话框中，单击注册。

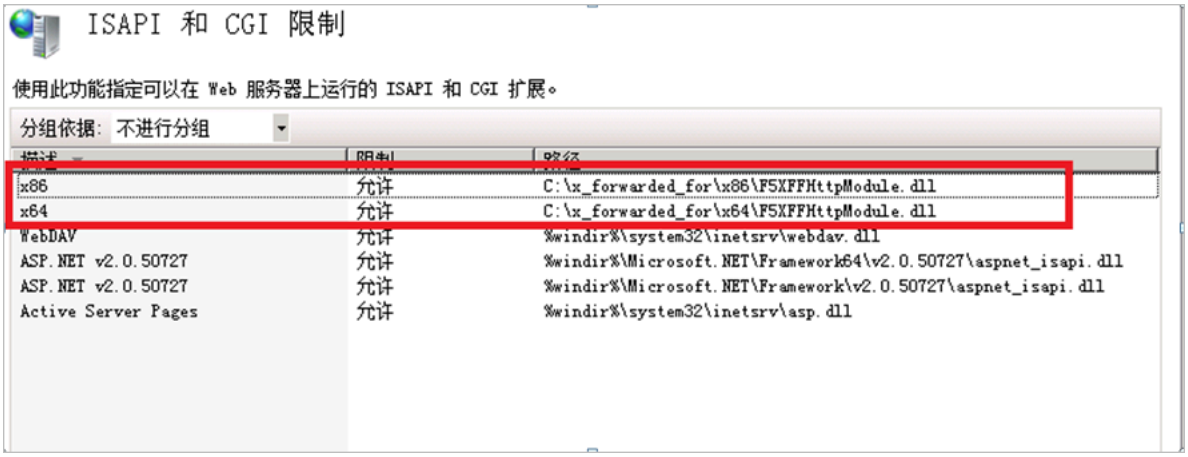


6. 添加已下载的 *F5XFFHttpModule.dll* 文件。

7. 添加完成后，选中刚才注册的模块，单击确定。



8. 在API 和CGI限制窗口添加 *F5XFFHttpModule.dll* 文件，并设置为允许。



9. 重启IIS服务器，配置生效。

Apache配置方案

Windows操作系统

在Apache 2.4及以上版本的安装包中已自带remoteip_module模块文件（mod_remoteip.so），您可以通过该模块获取访问者真实IP地址。

1. 在Apache的extra配置文件夹（*conf/extra/*）中，新建httpd-remoteip.conf配置文件。

说明:

为减少直接修改httpd.conf配置文件的次数，避免因操作失误而导致的业务异常，通过引入remoteip.conf配置文件的方式加载相关配置。

2. 在httpd-remoteip.conf配置文件中，添加以下访问者真实IP的获取规则。

```
#加载mod_remoteip.so模块
LoadModule remoteip_module modules/mod_remoteip.so
#设置RemoteIPHeader头部
RemoteIPHeader X-Forwarded-For
#设置回源IP段
RemoteIPInternalProxy 112.124.159.0/24 118.178.15.0/24 120.27.173.0
/24 203.107.20.0/24 203.107.21.0/24 203.107.22.0/24 203.107.23.0/24
47.97.128.0/24 47.97.129.0/24 47.97.130.0/24 47.97.131.0/24
```

3. 修改*conf/httpd.conf*配置文件，插入httpd-remoteip.conf配置文件。

```
Include conf/extra/httpd-remoteip.conf
```

4. 在httpd.conf配置文件中，修改日志格式。

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

5. 重启Apache服务，使配置生效。

Linux操作系统

您可以通过安装Apache的*mod_rpaf*第三方模块，获取访问者真实IP地址。

1. 执行以下命令，安装mod_rpaf模块。

```
wget http://stderr.net/apache/rpaf/download/mod_rpaf-0.6.tar.gz
tar zxvf mod_rpaf-0.6.tar.gz
cd mod_rpaf-0.6
/alidata/server/httpd/bin/apxs -i -c -n mod_rpaf-2.0.so mod_rpaf-2.0
.c
```

2. 修改Apache配置文件*/alidata/server/httpd/conf/httpd.conf*，在文件最后添加以下内容：

说明：

其中，`RPAFproxy_ips ip地址`不是负载均衡提供的公网IP。具体IP可参考Apache的日志，通常会有两个IP地址。

```
LoadModule rpaf_module modules/mod_rpaf-2.0.so
RPAFenable On
RPAFsethostname On
RPAFproxy_ips ip地址
```

```
RPAFheader X-Forwarded-For
```

3. 添加完成后，执行以下命令重启Apache服务，使配置生效。

```
/alidata/server/httpd/bin/apachectl restart
```

mod_rpaf模块配置示例

```
LoadModule rpaf_module modules/mod_rpaf-2.0.so
RPAFenable On
RPAFsethostname On
RPAFproxy_ips 10.242.230.65 10.242.230.131
RPAFheader X-Forwarded-For
```

Tomcat配置方案

开启 Tomcat 的 X-Forwarded-For 功能可获取客户端真实IP。

在 *tomcat/conf/server.xml* 文件中，修改 AccessLogValve 日志记录功能：

```
<Valve className="org.apache.catalina.valves.AccessLogValve" directory
="logs"
prefix="localhost_access_log." suffix=".txt"
pattern="%{X-FORWARDED-FOR}i %l %u %t %r %s %b %D %q %{User-Agent}i %T
" resolveHosts="false"/>
```

5.12 高防源站保护

不同场景下高防源站保护的方式和原理不同。 请参考本文介绍的场景，选择适合您当前架构的方式进行配置。

说明:

配置源站保护，并不能防止没有经过高防的流量对源站直接发起DDoS攻击（甚至将源站打进黑洞）。配置高防源站保护只针对小流量CC攻击以及Web攻击有防护意义，对于防护大规模DDoS攻击的意义并不大。

网站防护（七层转发）

- 高防IP > ECS或不在阿里云的源站

  在这种架构下，访问ECS、源站流量的源IP都会变成高防的回源IP。

  您可以使用源站上的安全软件（如iptables、防火墙等），只放行高防的回源IP，同时拦截其他所有来自非高防回源段的IP地址。

- 高防IP > SLB > ECS

  在这种架构下，访问ECS流量的IP变成SLB的IP。

建议您通过SLB的白名单功能来只允许高防IP访问SLB。

- 高防IP > WAF/CDN > ECS

  在这种架构下，访问ECS流量的IP会变成WAF或者CDN的IP，原理和SLB相同。

  如果条件允许，您可以在WAF、CDN配置相应策略，源站的策略则针对WAF或CDN的回源IP来配置。

非网站防护（四层转发）

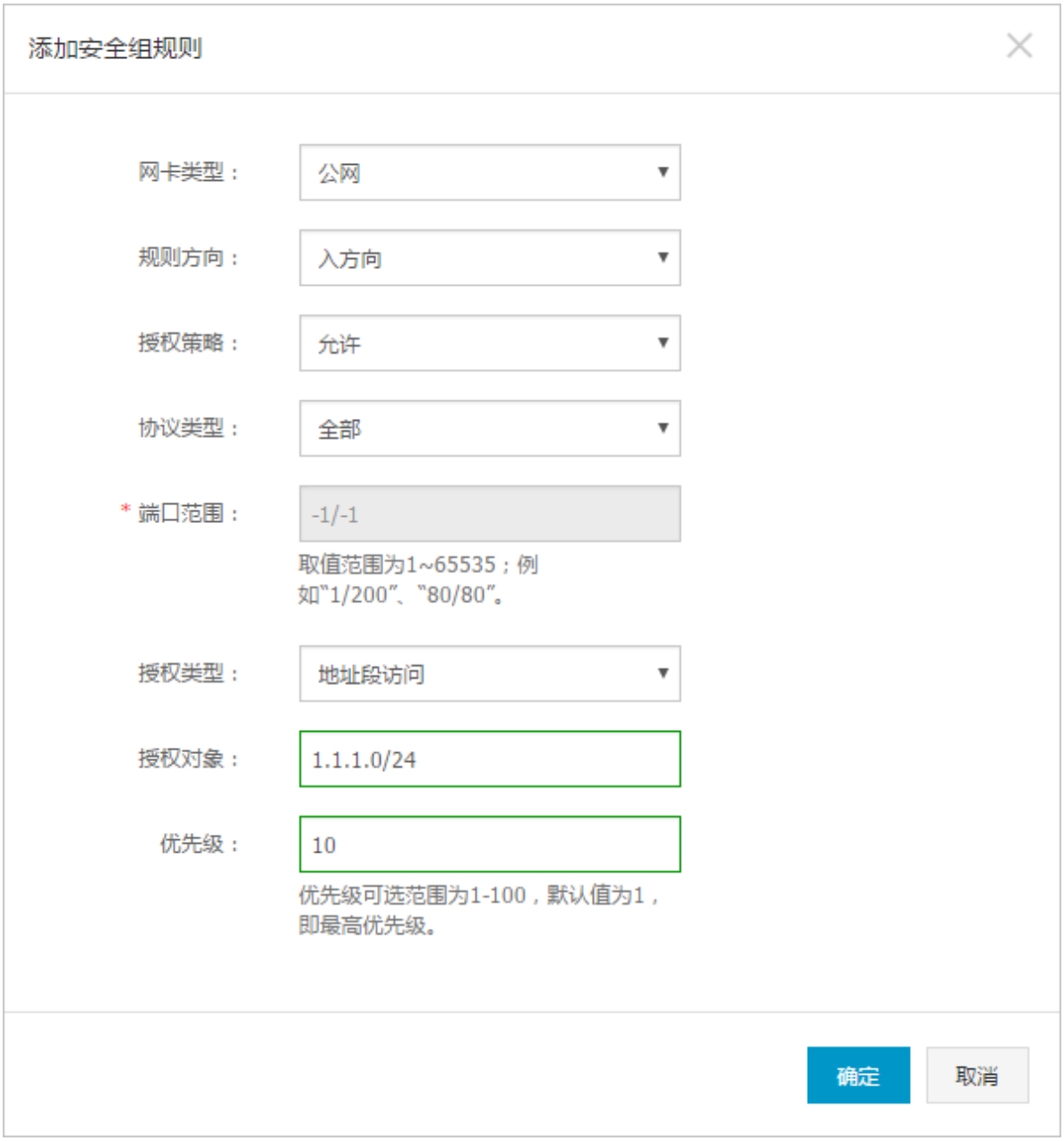
源站保护对四层转发无效。即使配置源站保护，如果攻击绕过高防IP直接攻击源站，还是会将源站的上游链路堵死或者引发黑洞，无法起到源站保护的效果。

设置ECS安全组保护源站

参照以下步骤，设置ECS安全组。

1. 登录到云服务器 *ECS* 控制台。
2. 从左侧导航栏选择安全组，并选择目标区域（安全组只能应用于相同区域下的ECS），单击创建安全组。
3. 填写安全组名称、描述等信息，单击确定。

4. 在新创建的安全组的操作列下，单击配置规则进入规则编辑页面，单击添加安全组规则。
5. 假设高防IP服务的回源IP段为`1.1.1.0/24`，您可以按如下示例添加安全组规则。



说明:

- **授权对象一次可添加一个IP或IP段。如果有多个IP或IP段，可通过添加多个规则实现。**
- **优先级高的规则，会优先匹配。**

6. **按照示例中放行全部高防回源IP段后，再添加一条优先级较低的规则拒绝所有IP访问。**
7. **配置完安全组规则后，找到需要放行高防回源IP的ECS实例，选择本实例安全组，单击加入安全组，将ECS实例加入该安全组。**

6 API参考

7 常见问题

7.1 BGP高防是什么？有什么优势？

BGP协议是什么？

边界网关协议，简称BGP，主要用于互联网AS（自治系统）之间的互联。BGP协议的最主要功能在于控制路由的传播和选择最好的路由。

BPG线路有以下功能特点：

- 单IP多线接入。通过BGP可以实现一个IP对应电信、联通、移动、长城、教育网等不同线路的带宽，而不需要服务器端配置多个IP。
- 使用BGP高防可以解决跨运营商访问慢、部分小运营商访问不稳定的情况。
- 从运营商网络质量来看，BGP带宽是中国大陆地域目前最昂贵的、线路质量也是最好的线路。对于延迟要求比较苛刻的业务（如即时对战游戏）也会优先选用BGP线路。

BGP线路有什么优势？

- 消除南北访问障碍。由于BGP可以将联通、电信、移动等运营商的线路“合并”，使得中国南北无障碍通讯成为可能。对接入层来说，可使“联通、电信”这类区别消失，更能使一个网站资源无限制的在全国范围内无障碍访问，而不需要在异地部署VPN或者异地加速站来实现异地无障碍访问。
- 高速互联互通。原来，一条线路访问另一线路往往要经过很多层路由，但实现BGP以后就像进入了高速公路。

  原来带宽的利用率一般在40%左右，实现BGP后能达到80%以上。因此，原来10M独享带宽的速度，通过BGP只需要5M就可以满足，提升效率的同时也节省了成本。

有了BGP为何还需要电信联通线路？

BGP线路资源宝贵，其基础防护带宽上限只有20G，而电信、联通线路的基础防护带宽最大可达300G（弹性防护带宽最大可达600G）。因此，建议使用联通+电信+BGP的三线套餐，可以在保证接入良好体验的同时，获得最大的防护能力。

BGP高防IP被黑洞了怎么办？

如购买单线BGP高防，黑洞后需要等待运营商自动解封，解封时间视攻击情况而定（如果攻击持续超过防护能力上限会持续黑洞），具体黑洞时间请参考阿里云黑洞策略。

如购买三线高防（BGP+电信+联通），并且启用了CNAME自动调度功能，BGP线路被黑洞后会自动把解析切换到电信和联通线路，保证业务的可用性。切换解析的动作秒级完成，具体解析生效的时间视DNS解析更新的实际时间而定。

BGP高防如何接入?

BGP高防接入方式与电信高防和联通高防相同，您购买BGP高防线路后会获得一个BGP高防IP。

1. 对于网站业务，您需要更改DNS解析到BGP高防IP。
2. 登录DDoS高防管理控制台，设置BGP高防IP的回源配置，添加需要转发的源站域名和IP。
3. 测试访问是否正常。

详细接入流程，请查看高防IP服务接入快速入门。

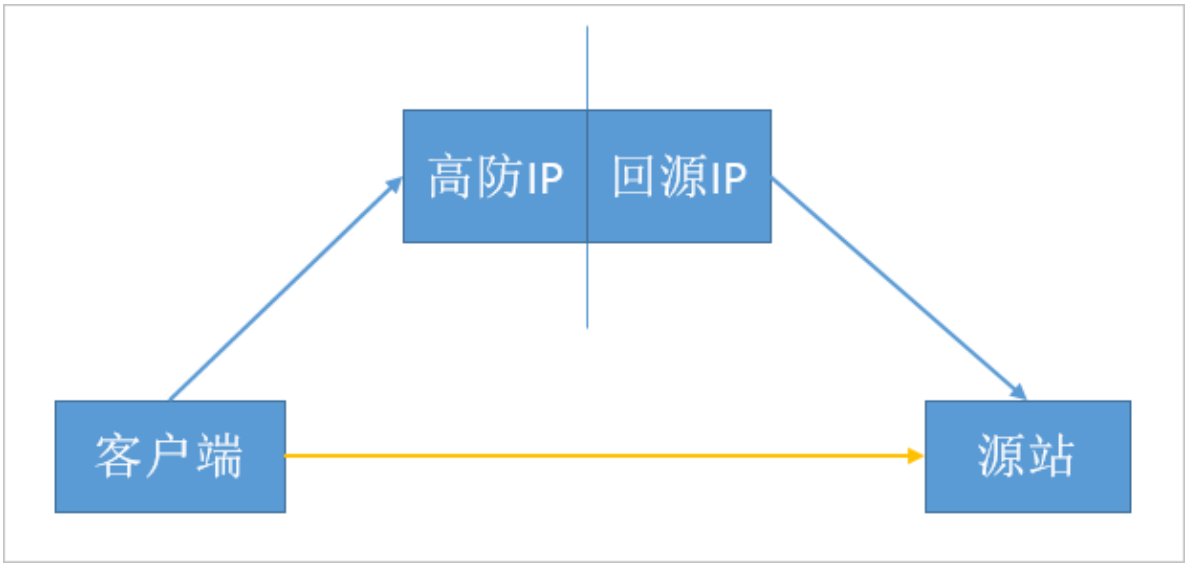
7.2 配置高防后访问网站，提示502错误

本文介绍了配置高防IP后，访问网站出现502报错的常见原因和解决方法。

高防回源IP被源站拦截或限速

- 高防回源IP

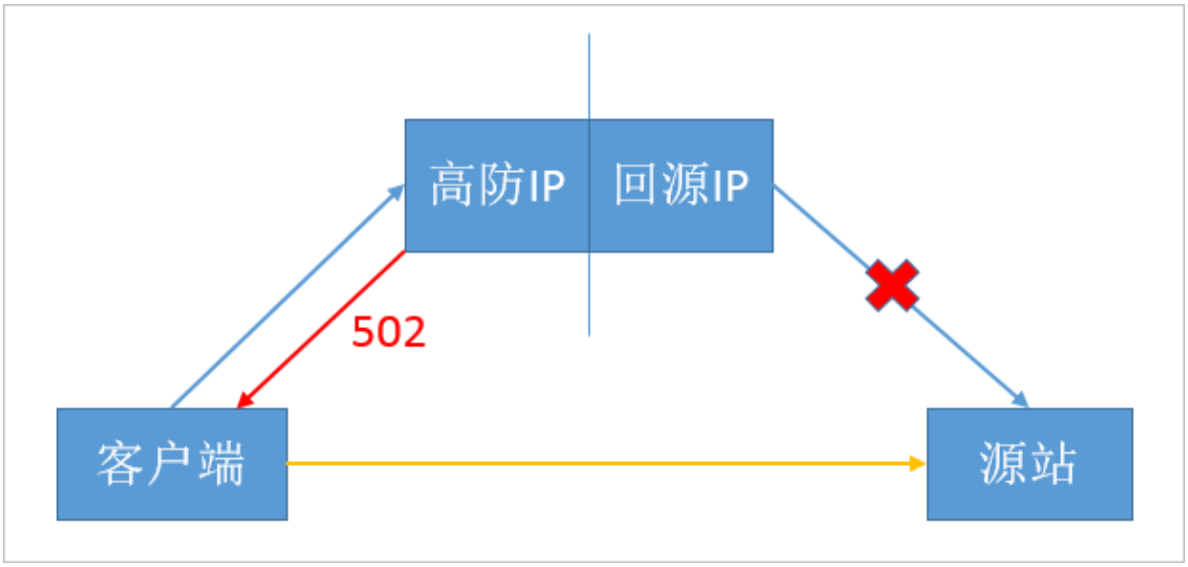
  在配置高防IP后，真实服务器（源站）的IP因为高防IP在中间代理而被隐藏。因此，在源站看来，所有经过高防IP服务访问的客户端源IP都会变成高防的回源IP。



  正常情况下，客户端请求访问高防IP，高防IP服务收到请求后把真实客户端的源IP转换成高防的回源IP（把真实客户端IP放在HTTP头部的X-Forwarded-For字段中）发送给源站。但是，如果源站IP暴露，客户端可以直接请求访问源站，这样就绕过了高防IP服务提供的防护。

- 为什么会被拦截或限速?

没有配置高防IP代理时，在源站看来真实客户端地址是非常分散的。正常情况下，每个源IP的请求量都不大。而配置高防IP服务后，高防回源的IP段固定且有限。因此，在源站看来所有的访问请求都来自高防回源IP段，分摊到每个回源IP上的请求量也会变大，导致源站可能误认为高防回源IP在对源站进行攻击。此时，源站如果有防御DDoS的安全策略，很可能会将回源IP拦截或者限速。



- 如何解决?

  根据上述原理，只要在源站放行所有的高防回源IP，即可解决出现的502错误。设置源站放行高防回源IP方法有两种：

  - 方法一：参考如何查看高防回源IP段获取高防回源IP，然后在您源站的防火墙、主机安全防护软件(如安全狗)中，将高防回源IP网段添加到白名单。
  - 方法二：直接关闭源站的防火墙及主机安全防护软件。

源站本身出现异常，导致响应高防的请求超时

源站本身异常包括以下情形：

- 源站IP暴露，被恶意攻击导致瘫痪。
- 源站服务器机房物理故障。
- 源站服务器中 Apache、Nginx 等Web程序出现问题。
- 服务器内存、CPU 占用过高，导致性能骤降。
- 源站上行链路拥挤阻塞。

判断方法

修改本机 hosts 文件，将域名直接指向源站IP。如果直接通过源站IP也不能访问，同时伴随 ping 源站IP丢包、telnet超时等现象，可判断为是此类原因导致。

排查方法

参照以下步骤进行排查：

1. 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。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。这种情况，建议您尽快更换源站IP。
2. 排除遭受攻击的原因后，可查看源站服务器的进程状态、CPU/内存占用情况、机房带宽的监控情况等。如有异常，建议您联系服务器相关技术人员或机房人员协助排查解决。
3. 如果是个别客户端出现502错误，建议您收集客户端的IP和出现异常的时间点，并提交工单，售后技术支持团队会对比相关日志协助您进行排查。

网络出现拥塞或抖动

在已经排除上述两种原因后，偶发的局部网络抖动、运营商线路故障等因素也可能导致502错误。您可提交工单反馈此情况，售后技术支持团队将为您提供链路质量监控的信息。

7.3 高防IP常见问题

本文档列举了高防 IP 服务相关的常见问题。您可以在问题列表中查找您想要了解的问题，并单击问题查看相关解答。

- 非阿里云用户可以使用高防IP吗？
- BGP高防是什么？
- 高防IP是否支持二线路升级三线路？
- 高防IP是否支持泛域名？
- 中国大陆地域网站业务接入高防IP是否需要ICP备案？
- 已购买20G基础防护带宽的高防IP实例，仍不够用，能否随时升级到更高的防护能力？
- 高防IP过期后会怎样？
- 高防IP服务带宽说明
- 购买高防IP业务带宽500Mbps后，是每个高防IP均拥有500Mbps业务带宽吗？
- 超过高防IP服务带宽会有什么影响？
- 高防IP被黑洞后，支持手动解封吗？
- 高防IP实例的状态显示为黑洞延迟中是什么意思？
- 高防IP(香港)备用IP的作用是什么？
- 如果DDoS高防（香港）主IP被黑洞了，是否整个高防IP都被黑洞了？
- 高防回源IP地址有哪些？

- 高防IP是否会自动将高防IP的回源地址加入安全组?
- 高防IP服务中的源站IP可以填写内网IP吗?
- 修改高防IP服务的源站IP是否有延迟?
- 在高防IP服务控制台中，更改配置后大约需要多少时间生效?
- 高防IP服务控制台中，如何查看攻击者IP信息?
- 高防攻击源IP数据保留时间?
- 高防IP服务的安全报表是否只能获取最近一个月的报表数据?
- 高防IP实例配置了多个网站业务，被攻击后如何查看是哪个网站受到攻击?
- 高防IP服务的CNAME调度规则是什么?
- 网站CNAME和非网站CNAME有什么区别?
- 高防IP是否支持健康检查?
- 高防IP配置多个源站时如何负载?
- 高防IP服务是否有抓包文件?
- 高防IP服务是否支持会话保持?
- 高防IP服务的会话保持是如何实现的?
- 高防IP的TCP默认连接超时时间是多少?
- 高防IP的HTTP/HTTPS默认连接超时时间是多少?
- 高防IP服务是否支持IPv6协议?
- 高防IP服务是否支持Websocket协议?
- 高防IP服务是否支持HTTPS双向认证?
- 老版本浏览器和安卓客户端无法正常访问HTTPS站点?
- 高防支持的SSL协议和加密套件有哪些?
- 高防支持的转发端口数及支持域名数?
- 服务器的流量未达到清洗阈值，为何安全报表中会出现清洗流量?
- 高防IP服务是否支持接入采用NTLM协议认证的网站防护?

非阿里云用户可以使用高防 IP 服务吗?

非阿里云用户也可以使用高防 IP 服务。

高防 IP 是公网回源，因此只要是公网路由可达的服务器，不论是在阿里云、或是其他的云、IDC 机房等环境，都可以使用高防 IP 服务。

BGP 高防是什么?

BGP 高防线路默认提供 20 Gbps 基础防护带宽及最大 100 Gbps 的弹性防护带宽（BGP线路的最大弹性防护带宽根据网络流量实时动态调整，有时可能会低于 100 Gbps），主要用于提升非电信联通的用户访问体验。

更多关于 BGP 高防的信息，请查看*BGP*高防是什么？有什么优势？

高防 IP 是否支持二线路升级三线路?

高防 IP 服务不支持线路升级。您可重新购买三线高防 IP，进行配置迁移。在确认原双线高防 IP 已无业务流量后，提交工单说明已购买三线高防 IP、业务已迁移，并申请原双线高防 IP 的退款。

高防 IP 是否支持泛域名?

高防 IP 服务网站防护支持泛域名配置，您在配置 CC 防护和 WAF 防护的时候可以使用泛域名。

泛域名解析是指利用通配符（星号）作为次级域名，以实现所有的次级域名均指向同一 IP。 例如，为 www.taobao.com 配置泛域名解析后，访问 *.taobao.com 都将解析到泛域名解析的 IP 。

中国大陆地域网站业务接入高防 IP 是否需要 ICP 备案?

是的，源站在中国大陆地域接入高防 IP 必须具备 ICP 备案。

更多相关信息，请查看高防*IP*是否需要网站备案接入。

已购买 20G 基础防护带宽的高防 IP 实例，仍不够用，能否随时升级到更高的防护能力?

您可以登录云盾*DDoS*防护管理控制台，在资产 > 实例列表中，随时调整弹性防护带宽来获得更大的 DDoS 防护能力，弹性防护带宽调整即时生效。

高防 IP 过期后会怎样?

高防 IP 过期后内无防御能力，但转发规则配置正常生效，流量超限将触发流量限速，可能导致随机丢包。可通过控制台来释放实例。

高防 IP 服务带宽说明

高防 IP 业务防护带宽为一个高防实例累计的正常流量（以 IN 流量或 OUT 流量的最大值为准），单位：mbps。您可登录云盾*DDoS*防护管理控制台，在资产 > 实例列表中随时升级您的高防 IP 实例的业务带宽，目前最高支持升级到 2G 业务带宽。

购买高防 IP 业务带宽 500Mbps 后，是每个高防 IP 均拥有 500Mbps 业务带宽吗?

所购买的业务带宽是针对整个高防实例的。比如您的高防实例有三个高防 IP，则三个高防 IP 的业务带宽累加不能超过 500Mbps。

超过高防 IP 服务带宽会有什么影响?

如果您的流量超过购买的业务防护带宽，将触发流量限速，可能导致随机丢包。

高防 IP 被黑洞后，支持手动解封吗?

目前，高防 IP 服务已支持部分线路的手动解封操作。每个高防 IP 服务用户每天拥有三次黑洞解封机会，超过三次后当天将无法进行解封操作。更多详情，请查看黑洞解封。

高防 IP 实例的状态显示为黑洞延迟中是什么意思?

如果您购买的高防 IP 实例非最高规格，当您的高防 IP 实例第一次遭受超过黑洞阈值的攻击时，您的高防 IP 将不会立刻进入黑洞，阿里云免费帮您延迟两个小时，黑洞延迟期间使用高达 120G 的弹性防护能力为您提供防御。

> 说明:
>
> - 对于每个高防 IP 实例，仅提供一次黑洞延迟服务。
> - 黑洞延迟期间，如果遭受的攻击超过 120G，您的高防 IP 仍将进入黑洞。
> - 黑洞延迟结束后，您的高防 IP 实例将恢复至您所购买规格的防护能力，如果攻击仍在持续且超过黑洞阈值，您的高防 IP 将立即进入黑洞。

高防 IP (香港) 备用 IP 的作用是什么?

当主 IP 所在机房发生故障、宕机等短时间内无法恢复的情况时，您可以使用备用 IP 进行灾备切换。为确保灾备切换顺畅，请保持备用 IP 与主 IP 配置同步。

> 说明:
> 主、备 IP 的防护能力是不一样的，请使用主 IP 防护您的业务。备 IP 仅作为灾备切换时使用，正常情况下不建议使用备用 IP。

如果DDoS高防（香港）主 IP 被黑洞了，是否整个高防 IP 都被黑洞了?

主 IP 被黑洞后，默认备用 IP 不会被黑洞。 但在这种情况下，高防 IP 服务不会自动将解析切换到备 IP。由于备用 IP 只有 500M 的防护能力，如果您将业务手动解析到备用 IP，攻击超过防护能力后，备用 IP 也会被黑洞。

高防回源 IP 地址有哪些?

您可以登录云盾*DDoS*防护管理控制台 中，查看详细的高防IP回源地址段。详细操作步骤，请参考如何查看高防回源*IP*段。

高防 IP 是否会自动将高防 IP 的回源地址加入安全组?

高防 IP 服务不会将高防回源 IP 段添加到安全组，您也不需要将高防回源 IP 段添加到您的 ECS 或 VPC 安全组。但是，如果您的源站部署了防火墙或其它主机安全防护软件，您需要将高防回源IP段添加至相应的白名单中。

高防 IP 服务中的源站 IP 可以填写内网 IP 吗?

高防 IP 是通过公网进行回源的，不支持直接填写内网 IP。

修改高防 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 后，需要大约五分钟生效，建议您在业务低峰期进行变更操作。

在高防 IP 服务控制台中，更改配置后大约需要多少时间生效?

一般情况下，更改后的配置在5-10分钟即可生效。

高防 IP 服务控制台中，如何查看攻击者 IP 信息?

您可以在高防 IP 服务控制台中的安全报表中查看攻击者 IP 等相关攻击信息。

高防攻击源 IP 数据保留时间?

高防攻击源 IP 数据保留 30 天，建议您在高防 IP 服务的安全报表中及时获取相关数据。

高防 IP 服务的安全报表是否只能获取最近一个月的报表数据?

目前高防 IP 服务的安全报表不支持获取更早的数据，建议您及时获取对应的安全报表。

高防 IP 实例配置了多个网站业务，被攻击后如何查看是哪个网站受到攻击?

针对高防 IP 的大流量 DDoS 攻击行为，从数据包层面是无法分辨具体攻击哪个网站业务的。建议您使用多组高防 IP 实例，将您的网站分别部署在不同的高防 IP 实例上即可查看各个网站遭受攻击的情况。

高防IP服务的 CNAME 调度规则是什么?

当某个高防 IP 进入黑洞之后，CNAME 自动调度功能将随机地将该高防 IP 的流量调度至其它高防线路 IP，且生效时间也依赖于 LDNS 的缓存更新时间。

说明:

需要开启 CNAME 自动调度功能。

非网站如何使用CNAME域名调度?

网站 CNAME：每个域名产生一个独立的 CNAME，且具备黑洞后的自动调度能力。

说明:

如果满足以下条件，非网站配置可以通过网站的 CNAME 实现自动调度功能。

- 三条线路的非网站转发的配置一致。
- 应用本身调用支持域名调用。

在这种情况下，您可以配置一个网站接入（如forward.example.com），并使用该网站配置产生的 CNAME 供非网站转发使用，即可实现 CNAME 自动调度功能。

高防 IP 是否支持健康检查?

网站业务默认开启健康检查。关于高防 IP 的健康检查工作原理，参考 SLB 服务的健康检查原理。

非网站业务默认不开启健康检查，但可以通过控制台来开启，操作步骤请参考高防健康检查配置。

高防 IP 配置多个源站时如何负载?

- 网站业务通过源地址 hash 方式进行负载均衡。
- 非网站业务可通过加权轮询（wrr）的方式轮询转发，负载权重为 1:1:1。

高防 IP 服务是否有抓包文件?

电信和联通线路高防 IP 服务不支持下载抓包文件，您可在云盾管理控制台直接查看攻击源 IP 信息。

针对 BGP 高防 IP 服务，您可以通过工单，提供相关 IP 及黑洞时间，索取攻击时的采样抓包文件。

高防 IP 服务是否支持会话保持?

高防 IP 服务支持会话保持，默认不开启。非网站可以通过控制台进行配置操作，请参考高防配置会话保持规则。

高防 IP 服务的会话保持是如何实现的?

开启会话保持后，在会话保持的设定期间内，高防 IP 服务会把同一 IP 的请求持续发往源站中的一台服务器。但是，如果客户端的网络环境发生变化（比如，从有线切成无线、4G 网络切成无线等），由于 IP 变化会导致会话无法保持。

高防 IP 的 TCP 默认连接超时时间是多少?

高防 IP 的 TCP 默认连接超时时间为 900s。非网站可以通过控制台进行配置操作，请参考高防配置会话保持规则。

高防IP的 HTTP / HTTPS 默认连接超时时间是多少?

高防 IP 的 HTTP / HTTPS 默认连接超时时间为 120s。

高防 IP 服务是否支持 IPv6 协议?

高防 IP 服务暂时不支持 IPv6 协议。

高防 IP 服务是否支持 Web socket 协议?

高防 IP 服务中的网站业务支持 Web socket 协议。请参考高防*websocket*配置。

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，支持 HTTPS 双向验证。

老版本浏览器和安卓客户端无法正常访问 HTTPS 站点?

请确认客户端是否支持 SNI 认证。 关于 SNI 认证可能引发的问题，请查看*SNI*可能引发的*HTTPS*访问异常。

高防支持的 SSL 协议和加密套件有哪些?

支持的 SSL 协议

- TLSv1
- TLSv1.1
- TLSv1.2

支持的加密套件

- ECDHE-ECDSA-AES128-GCM-SHA256
- ECDHE-ECDSA-AES256-GCM-SHA384
- ECDHE-ECDSA-AES128-SHA256
- ECDHE-ECDSA-AES256-SHA384
- ECDHE-RSA-AES128-GCM-SHA256
- ECDHE-RSA-AES256-GCM-SHA384
- ECDHE-RSA-AES128-SHA256
- ECDHE-RSA-AES256-SHA384
- AES128-GCM-SHA256
- AES256-GCM-SHA384
- AES128-SHA256
- AES256-SHA256
- ECDHE-ECDSA-AES128-SHA
- ECDHE-ECDSA-AES256-SHA

- ECDHE-RSA-AES128-SHA
- ECDHE-RSA-AES256-SHA
- AES128-SHA
- AES256-SHA
- DES-CBC3-SHA
- RSA+3DES

高防支持的转发端口数及支持域名数?

- 转发端口数：TCP/UDP协议转发支持条目数，默认为50个每IP，最大可扩展至200个每IP
- 支持域名数：HTTP/HTTPS转发支持条目总数，默认为50条每实例，最大可扩展至200条每实例

服务器的流量未达到清洗阈值，为何安全报表中会出现清洗流量?

对于已接入DDoS高防IP服务的业务，高防IP将自动过滤网络流量中存在的一些畸形包（例如，SYN小包、SYN标志位异常等不符合TCP协议的数据包），使您的业务服务器无需浪费资源处理这些明显的畸形包。这类被过滤的畸形包也将被计入清洗流量中，因此即使您的服务器流量未达清洗阈值，仍可能出现清洗流量。

高防IP服务是否支持接入采用NTLM协议认证的网站防护?

高防IP服务不支持接入使用NTLM协议认证的网站，经高防转发的访问请求可能无法通过源站服务器的NTLM认证，客户端将反复出现认证提示。

建议您的网站采用其他方式进行认证。

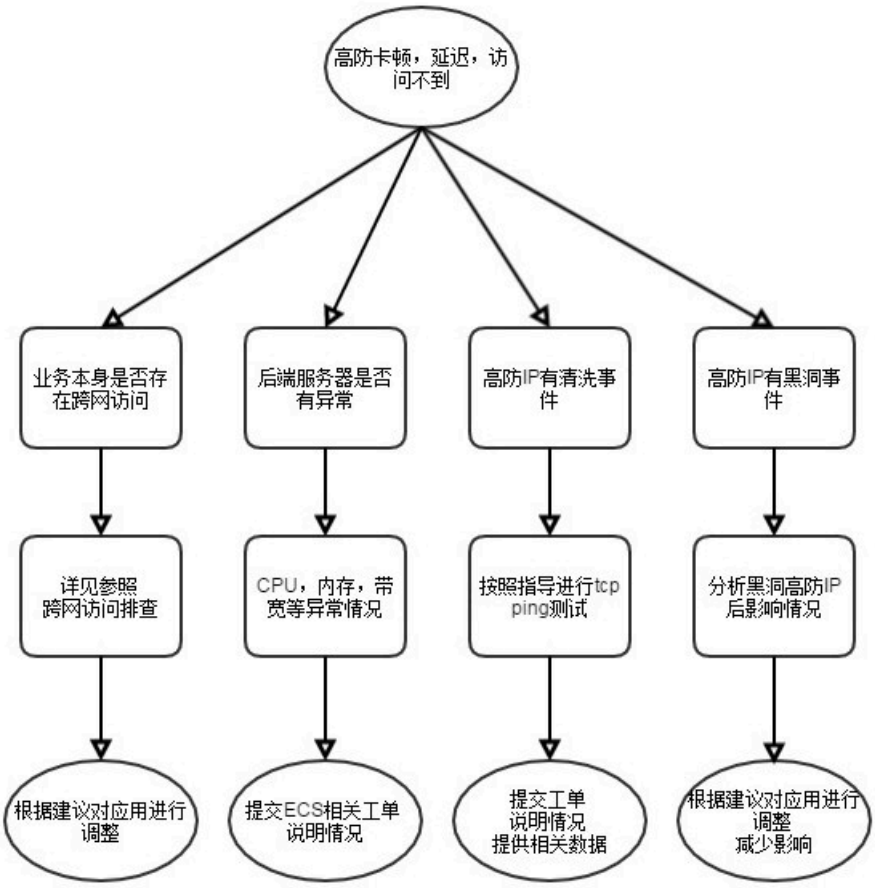
7.4 高防IP卡顿、延迟、访问不通等问题排查

问题描述

客户端访问高防IP异常卡顿，出现较大延迟、丢包现象。

分析思路

遇到此类问题时，建议您收集受影响的客户端源IP，并通过 Traceroute 信息或 MTR 命令等工具进行链路测试，来判断问题来源。



排查方法

- **业务本身是否存在跨网访问**

  高防IP服务支持电信、联通、及BGP三种线路。其中，BGP线路用于优化移动及小运营商网络质量。

  - **当非电信（如联通，移动等）用户端跨网访问电信线路时，存在一定延迟和丢包。**
  - **当非联通（如电信，移动等）用户端跨网访问联通线路时，存在一定延迟和丢包。**

  优化建议：电信用户端通过电信线路访问，联通用户端通过联通线路访问，移动及其他线路通过BGP线路访问。

- **后端服务器是否有异常**

  根据出现异常的高防IP配置的源站类型进行排查。

  - **源站是负载均衡（SLB）**

    参照以下步骤进行排查。

    1. 针对负载均衡IP和端口，通过运行 tcping 工具，查看记录是否有异常。

    2. 查看负载均衡服务器状态（如连接数情况、后端服务器）是否有异常状态。

3. 查看负载均衡是否设置黑、白名单，或者其他的访问控制策略，确认放行高防本身回源IP段。
4. 查看负载均衡后端ECS、VPC，确认是否有安全软件或其它IP封禁策略。

   
   说明:
   配置负载均衡(SLB)后，后端服务器无法看到访问真实源IP。如果有安全软件进行恶意IP识别并阻断，一般情况都是高防集群本身的回源IP，而此类IP都需要放行。
5. 查看负载均衡IP是否暴露。

- 源站是云服务器（ECS/VPC）

  参照以下步骤进行排查。

  1. 针对服务器IP和端口，通过运行 tcping 工具查看记录是否有异常。
  2. 查看后端服务器是否有异常事件，如服务器本身黑洞及清洗事件、CPU高、数据库请求慢、出方向带宽满等。
  3. 查看服务器本身是否设置黑、白名单，或者其他的访问控制策略，确认放行高防本身回源IP段。
  4. 查看ECS服务器或VPC，确认是否有安全软件或其它IP封禁策略阻断高防回源IP。
  5. 查看服务器IP是否暴露。

- 源站是非阿里云服务器

  参照以下步骤进行排查。

  1. 针对服务器IP和端口，通过运行 tcping 工具查看记录是否有异常。
  2. 查看服务器是否有异常事件，如CPU高、数据库请求慢、出方向带宽满等。
  3. 查看服务器本身是否设置黑、白名单，或者其他的访问控制策略，确认放行高防本身回源IP段。
  4. 查看服务器，确认是否有安全软件或其它IP封禁策略阻断高防回源IP。

     
     说明:
     非阿里云服务器一般都无法识别访问真实源IP，如果有安全软件进行恶意IP识别并阻断，一般情况都是高防集群本身的回源IP，而此类IP都需要放行。
  5. 查看服务器IP是否暴露。

     
     说明:
     配置高防IP服务后，建议您更换后端源站服务器IP，不要使用之前已暴露的IP。

如果您使用的是阿里云产品，发现异常并需售后技术支持团队协助进行排查，请提交相关云产品工单，并说明情况。

- 高防IP是否有清洗事件
  - 高防IP有清洗事件

    参照以下步骤进行排查。

    1. 针对受攻击端口，通过运行 tcping 工具查看是否有延迟和丢包，并记录。
    2. 针对未被攻击端口，通过运行 tcping 工具查看是否有延迟和丢包，并记录。

    根据记录结果，对照下表查看问题原因。

受攻击端口是否有延时、丢包	未被攻击端口是否有延时、丢包	问题原因分析
是	否	说明清洗策略未误杀，查看后端服务器状态是否异常，确认后端服务器抗攻击性能。若服务器抗攻击能力较弱，则需要收紧防御策略。
是	是	清洗策略误杀导致。请提交工单，需要进行后端排查。
否	否	非清洗策略原因。
否	是	一般不存在这种情况。

    上述前两种情况，建议您通过工单说明情况，并提交售后技术支持团队来协助您处理。若需要收紧防御策略，您需要提供服务器抗攻击能力的详细参数，包括：

    ■ 正常用户访问情况
    ■ 业务主要交互过程
    ■ 应用对外服务能力

  - 高防IP没有清洗事件

    说明问题非攻击导致。

- 高防IP有黑洞事件

  在有黑洞事件时，请确认进入黑洞的IP，以及受影响访问是否都经过该IP。在一定条件下，高防IP被黑洞后具备自动切换功能，但客户端实际生效时间依赖于DNS解析、本地DNS缓存和更新时间。

  - 网站接入

在高防IP > 网站页面，确认是否开启CNAME自动调度功能。CNAME自动调度可以确保当某个线路的高防IP出现问题时，自动把业务切换到其他正常的线路，提供灾备能力，保证业务的连续性和可用性。

■ 当电信线路的IP被黑洞时，可以自动摘除电信IP的解析，只解析到联通和BGP线路。

■ 当联通线路的IP被黑洞时，可以自动摘除联通IP的解析，只解析到电信和BGP线路。

■ 当BGP线路的IP被黑洞时，可以自动摘除BGP IP的解析，只解析到电信和联通线路。

- 非网站接入

非网站接入方式没有CNAME切换调度逻辑，请确认是否自身进行调度。

建议：对应用进行调整，使其具备切换能力。当线路被黑洞时，可切换至正常线路。

· 其他

若问题仍未解决，请提交工单联系售后技术支持团队。为便技术支持团队快速判断及分析问题，请在工单内提供以下访问情况信息。

线路	影响访问源IP	被访问高防IP	Ping信息	traceroute或mtr信息	tcping或端口连接信息
电信线路	例如：1.1.1.1	例如：180.97.163.0	提供连续且大于10次 ping 请求的结果。	提供从此访问源IP至被访问高防IP的 tracert 或 traceroute 信息。	提供连续且大于10次的 tcpping 或端口连接信息。
联通线路	…	…	…	…	
BGP线路	…	…	…	…	

您也可以在工单中补充以下信息，方便售后技术支持团队快速定位问题：

- 高防IP配置回源IP的类型，如负载均衡、云主机（ECS/VPC）、非阿里云服务器。
- 回源IP，及负载均衡、云主机（ECS/VPC）、或非云阿里云服务器的日志，如CPU、内存、带宽、连接数等数据。
- 源站是否存在访问控制策略。
- 源站是否有安装安全软件，如云锁、360、安全狗、自带iptables等。
- 源站是否有安全策略，如针对IP级别的检测及过滤。
- 高防IP是否有清洗及黑洞事件。
- 业务类型，如网站、端游、页游、APP等。
- 问题出现时间，是否有其他涉及更改、删除高防IP实例的操作。

常用检查工具的使用及介绍

Traceroute 命令行工具

Traceroute 是 Linux 预装的网络测试工具，用于跟踪 Internet 协议（IP）数据包传送到目标地址时经过的路径。

Traceroute 会发送具有最大存活时间值（Max_TTL）的 UDP 探测数据包，然后侦听从网关开始的整个链路上的 ICMP TIME_EXCEEDED 响应。探测从 TTL=1 开始，TTL 值逐步增加，直至接收到 ICMP PORT_UNREACHABLE 消息。ICMP PORT_UNREACHABLE 消息用于标识目标主机已经被定位，或命令已经达到允许跟踪的最大 TTL 值。

说明:

Traceroute 默认发送 UDP 数据包进行链路探测。您可以使用 -I 参数来指定发送 ICMP 数据包用于探测。

示例

```
[root@centos ~]# traceroute -I 223.5.5.5
traceroute to 223.5.5.5 (223.5.5.5), 30 hops max, 60 byte packets
 1  * * *
 2  192.168.17.20 (192.168.17.20)  3.965 ms  4.252 ms  4.531 ms
 3  111.1.20.41 (111.1.20.41)  6.109 ms  6.574 ms  6.996 ms
 4  111.1.34.197 (111.1.34.197)  2.407 ms  2.451 ms  2.533 ms
 5  211.138.114.25 (211.138.114.25)  1.321 ms  1.285 ms  1.304 ms
 6  211.138.114.70 (211.138.114.70)  2.417 ms 211.138.114.66 (211.138.
114.66)  1.857 ms 211.138.114.70 (211.138.114.70)  2.002 ms
 7  42.120.244.194 (42.120.244.194)  2.570 ms  2.536 ms 42.120.244.186
 (42.120.244.186)  1.585 ms
 8  42.120.244.246 (42.120.244.246)  2.706 ms  2.666 ms  2.437 ms
 9  * * *
10  public1.alidns.com (223.5.5.5)  2.817 ms  2.676 ms  2.401 ms
```

更多关于 Traceroute 命令行工具的信息，请查看链路测试工具使用及介绍。

TRACERT 命令行工具

TRACERT (Trace Route) 是 Windows 自带的网络诊断命令行实用程序，用于跟踪 Internet 协议 (IP) 数据包传送到目标地址时经过的路径。

TRACERT 通过向目标地址发送 ICMP 数据包来确定到目标地址的路由。在这些数据包中，TRACERT 使用不同的 IP “生存期” (TTL) 值。由于要求沿途的路由器在转发数据包前至少必须将 TTL 减少 1，因此 TTL 实际上相当于一个跃点计数器 (hop counter)。当某个数据包的 TTL 达到零 (0) 时，相应节点就会向源计算机发送一个 ICMP “超时” 消息。

TRACERT 第一次发送 TTL 为 1 的数据包，并在每次后续传输时将 TTL 增加 1，直到目标地址响应或达到 TTL 的最大值。中间路由器发送回来的 ICMP “超时” 消息中包含了相应节点的信息。

样例

```
C:\> tracert -d 223.5.5.5
通过最多 30 个跃点跟踪到 223.5.5.5 的路由

  1     *        *        *     请求超时。
  2     9 ms     3 ms    12 ms  192.168.17.20
  3     4 ms     9 ms     2 ms  111.1.20.41
  4     9 ms     2 ms     1 ms  111.1.34.197
  5    11 ms     *        *     211.140.0.57
  6     3 ms     2 ms     2 ms  211.138.114.62
  7     2 ms     2 ms     1 ms  42.120.244.190
  8    32 ms     4 ms     3 ms  42.120.244.238
  9     *        *        *     请求超时。
 10     3 ms     2 ms     2 ms  223.5.5.5

跟踪完成。
```

更多关于 TRACERT 命令行工具的信息，请查看链路测试工具使用及介绍。

TCPing工具

TCPing工具使用TCP的方式去查看端口情况，可以检测出TCP延迟及连接情况。下载*TCPing*工具。

- Windows使用方法

  将TCPing工具拷贝至 Windows 指定目录，在命令提示行中运行`tcping www.aliyun.com 80`。

  样例

  ```
  C:\>tcping.exe www.aliyun.com 80

  Probing 140.205.62.8:80/tcp - Port is open - time=19.550ms
  Probing 140.205.62.8:80/tcp - Port is open - time=8.761ms
  Probing 140.205.62.8:80/tcp - Port is open - time=10.899ms
  Probing 140.205.62.8:80/tcp - Port is open - time=13.013ms

  Ping statistics for 140.205.62.8:80
       4 probes sent.
       4 successful, 0 failed.
  Approximate trip times in milli-seconds:
       Minimum = 8.761ms, Maximum = 19.550ms, Average = 13.056ms
  ```

- Linux使用方法

  运行以下命令，安装tcping工具。

  ```
  tar zxvf tcping-1.3.5.tar.gz
  cd tcping-1.3.5
  ```

```
make tcping.linux
```

参照以下样例，来使用tcping工具。

```
[root@aliyun tcping-1.3.5]# for ((i=0; i<10; ++i)) ; do ./tcping
www.aliyun.com 80;done
www.aliyun.com port 80 open.
www.aliyun.com port 80 open.
www.aliyun.com port 80 open.
www.aliyun.com port 80 open.
www.aliyun.com port 80 open.
www.aliyun.com port 80 open.
www.aliyun.com port 80 open.
www.aliyun.com port 80 open.
www.aliyun.com port 80 open.
www.aliyun.com port 80 open.
```

7.5 配置高防后访问网站提示504错误

配置高防 IP 服务后，网站执行某些 POST 请求时，长时间等待后返回 504 错误，执行不成功。

问题原因

此问题是由于请求处理时间过长，已超过高防 IP 服务的连接阈值，高防 IP 服务主动断开连接。

- TCP 默认连接超时时间为 900s。
- HTTP / HTTPS 默认连接超时时间为 120s。

解决方法

建议您在应用层面部署长时间任务执行的心跳机制，确保在请求等待的过程中保持该连接活跃。

对于非常规偶发性任务请求，您可以绕过高防 IP 直接访问后端 ECS 云服务器执行该任务。

7.6 如何查看高防回源IP段

为了防止您的高防回源IP段被源站拦截或限速，您可以将高防回源 IP 段添加至您源站的防火墙，或其它主机安全防护软件的白名单中。

参照以下步骤，来查看高防回源IP段。

1. 登录云盾*DDoS*防护管理控制台。
2. 前往接入 > 网站。
3. 单击页面右上角高防回源IP段，查看您的高防 IP 实例的回源 IP 段。
4. 根据您使用的线路，将对应的高防回源IP段添加至您源站的防火墙，或其它主机安全防护软件的白名单中。

7.7 弹性计费常见问题

本文列举关于DDoS高防IP服务弹性计费的常见问题。

- BGP线路支持弹性防护吗？最大防护能力是多大？
- 如果购买弹性防护，一个月都没有攻击，是不是不需要任何费用？
- 我购买了20G的基础防护、50G的弹性防护，最终我的防护能力是多大？
- 超过弹性防护能力上限会怎样？
- 购买50G的弹性防护，实际攻击流量只有30G，如何收费？
- 当前选择的弹性防护带宽是100G，发现不够用，可以改成200G吗？
- 一个IP一天内被攻击多次，费用该怎么计算？
- 购买了双线套餐，电信和联通IP都受到了攻击，是按照攻击最大值收费吗？
- 购买了高防实例，如何停止使用弹性防护能力，避免产生弹性防护的后付费费用？

BGP线路支持弹性防护吗？最大防护能力是多大？

BGP线路支持最大100G的弹性防护带宽。您可以登录云盾DDoS防护管理控制台，在高防IP > 实例列表中为您已购买的BGP高防线路设置弹性防护带宽。

> 说明：
> 由于公网BGP带宽资源有限，BGP线路的弹性防护带宽部分有时可能无法达到您所设置的最大带宽。若当日未达到您所选择的弹性防护带宽的防御能力，您可以申请免除当日产生的弹性防护费用。

如果购买弹性防护，一个月都没有攻击，是不是不需要任何费用？

这种情况下，仅需要支付基础防护带宽的包月费用，不产生其它额外的费用。

> 说明：
> 如果业务流量超过了高防IP服务的规格（阿里云内200Mbps，云外100Mbps），还需要支付相应的流量费用。

我购买了20G的基础防护、50G的弹性防护，最终我的防护能力是多大？

最终实际防护能力为50G，以弹性防护能力为准。例如，假如您选择20G的弹性防护能力，最多只能提供20G的防护能力，相当于没有弹性防护功能。

超过弹性防护能力上限会怎样？

如果攻击流量超过防护能力，该IP会强制进入黑洞，阻断全部流量。

购买50G的弹性防护，实际攻击流量只有30G，如何收费？

攻击流量小于20G（基础防护）的部分不额外计费，只按照峰值收取30G攻击防护的费用。如实际攻击流量为30G，则弹性防护费用为1,787元。

DDoS攻击防御峰值	CC攻击防御峰值	弹性防护费用（天）
攻击峰值≤20Gb	攻击峰值≤60,000QPS	按规格包月
20Gb <攻击峰值≤30Gb	60,000QPS<攻击峰值≤100,000QPS	1,787
30Gb <攻击峰值≤40Gb	100,000QPS<攻击峰值≤130,000QPS	3,120
40Gb <攻击峰值≤50Gb	130,000QPS<攻击峰值≤160,000QPS	4,453
50Gb <攻击峰值≤60Gb	160,000QPS<攻击峰值≤200,000QPS	5,787
60Gb <攻击峰值≤70Gb	200,000QPS<攻击峰值≤230,000QPS	9,120
70Gb <攻击峰值≤80Gb	230,000QPS<攻击峰值≤260,000QPS	11,120
80Gb <攻击峰值≤100Gb	260,000QPS<攻击峰值≤300,000QPS	13,120
100Gb <攻击峰值≤150Gb	300,000QPS<攻击峰值≤450,000QPS	16,453
150Gb <攻击峰值≤200Gb	450,000QPS<攻击峰值≤600,000QPS	19,120
200Gb <攻击峰值≤300Gb	600,000QPS<攻击峰值≤1,000,000QPS	24,453

当前选择的弹性防护带宽是100G，发现不够用，可以改成200G吗？

可以。DDoS高防IP管理控制台支持调整弹性防护带宽，调大或者调小都可以。

说明：
当日发生的攻击已经计费，修改后次日将以最新的弹性带宽进行计费。

一个IP一天内被攻击多次，费用该怎么计算？

以当天（0:00-24:00）攻击的峰值为准，只收取一次。例如某IP一天内分别遭到50G、100G、200G共三次攻击，则当天的弹性防护付费账单按照200G攻击的弹性计费标准收取，即19,120元。

购买了双线套餐，电信和联通IP都受到了攻击，是按照攻击最大值收费吗？

计费是以单个IP为单位，而不是高防实例。因此，需要分别基于两个IP被攻击的最大值收取弹性防护费用。

购买了高防实例，如何停止使用弹性防护能力，避免产生弹性防护的后付费费用？

您可以将您购买的高防实例的弹性防护带宽设置为与基础防护带宽一致，在遭受到超出基础防护带宽流量的攻击时，将不会启用弹性防护带宽进行防护。

您可以登录云盾DDoS高防IP管理控制台，在资产 > 实例列表中，调整您已购买的高防实例的弹性防护带宽。

7.8 配置高防后网站上传大文件失败

配置高防 IP 服务后，在网站上传大文件时失败，并返回 413 错误。

问题原因

此问题是由于配置高防 IP 服务后，在防护网站上传文件最大不能超过 300 MB。

解决方法

- 方法一

  将文件压缩后再进行上传，确保需要上传的文件小于 300 MB。

- 方法二

  建议您将大文件存储在阿里云 OSS 的存储空间，而不是直接上传至源站 ECS 服务器。

- 方法三

  对于非常规偶发性的上传需求，您可以通过绑定 HOST 地址绕过高防 IP 直接访问 ECS 云服务器进行上传。

7.9 高防IP与安全组规则设置问题

当使用非网站 接入且源站为阿里云ECS或VPC 时，如果您的高防 IP 服务回源 ECS 的安全组中，设置了“只允许高防回源网段放行，并禁止其他所有网段”的规则，此规则可能导致访问客户端的真实IP被 ECS 安全组阻断。

问题原因

在最新版本的安全组中，其获取到的源地址是真实访问者的 IP。因此，禁止其他所有网段访问的规则将阻断正常访问流量。

解决方案

根据真实访问者 IP 重新设置 ECS 安全组规则。

示例

真实源 IP （1.1.1.1）-> 高防 IP （2.2.2.2）-> 高防回源 IP （3.3.3.3）-> ECS

如果您在 ECS 安全组设置了只允许 IP 为 3.3.3.3 通过，则您需要删除这条规则，并根据您的实际情况决定是否允许一些真实源 IP 通过。

7.10 SNI可能引发的HTTPS访问异常

什么是SNI?

随着 IPv4 地址的短缺，为了让多个域名复用一个 IP，在 HTTP 服务器上引入了虚拟主机的概念。服务器可以根据客户端请求中不同的 host，将请求分发给不同的域名（虚拟主机）来处理。

但是，在一个被多个域名（虚拟主机）共享 IP 的 HTTPS 服务器中，由于在握手建立之前服务器无法知道客户端请求的是哪个 host，所以无法将请求交给特定的虚拟主机。然而，要完成握手，又必须读取虚拟主机中配置的证书信息。

Server name indication（简称，SNI）就是用来解决这个矛盾问题的。SNI 要求客户端在与服务器握手时就携带需要访问的域名的 host 信息。这样，服务器就知道需要用哪个虚拟主机的证书与客户端握手并建立 TSL 连接。

SNI 最早在 2004 年被提出，目前主流的浏览器、服务器和测试工具都已支持 SNI。

为什么使用高防 IP / WAF 必须要求客户端支持 SNI?

高防 IP 和 WAF 服务在反向代理 HTTPS 业务时，需要代理客户端去和真实服务器（RS）进行交互，所以需要在配置 HTTPS 防护时上传证书和私钥。真实的高防 IP 和 WAF 服务器的数量是有限的，面对数以万计的域名显然无法实现一个域名一台物理服务器的配置，所以整个高防 IP 和 WAF 服务集群必然存在多个域名复用相同的服务器。因此，客户端必须支持 SNI，才能与高防 IP 和 WAF 进行正常交互。

如果使用不支持 SNI 的浏览器访问高防IP 或 WAF 服务防护的网站，高防 IP 和 WAF 因无法确认客户端请求的是哪个域名，无法调取对应的虚拟主机证书与客户端交互，只能使用内置的缺省证书与客户端连接。在这种情况下，在客户端浏览器上会出现“服务器证书不可信”的提示。

> 说明:
> 即使真实服务器只有一个域名（没有复用 IP 的情况），由于高防 IP 或 WAF 服务需要在中间进行反向代理，而客户端必须先与高防 IP 或 WAF 建立连接，所以客户端依然需要支持 SNI。

解决方案

服务器端

配置您的服务器，使其支持 SNI。

具体请参考:

- Nginx 服务器：同一个*IP*上配置多个*HTTPS*主机
- Apache 服务器：*apache mod_gnutls*实现多*HTTPS*虚拟主机

客户端

对于不支持 SNI 的客户端，建议您采用以下解决方案：

- 建议您的用户使用新版本的浏览器，如 Google Chrome、Firefox 等。
- 不要在高防 IP 服务中配置七层网站防护，而只采用四层 443 端口转发的方式配置网站防护。

> 说明:
> 配置采用四层防护将无法防护 CC 攻击。

SNI 兼容性

> 说明:
> SNI 兼容 TLS 1.1及以上的协议，但与 SSL 协议不兼容。

SNI 支持以下客户端-桌面版浏览器：

- Chrome 5 及以上版本
- Chrome 6 及以上版本
- Firefox 2 及以上版本
- Internet Explorer 7 及以上版本（仅支持 Windows Vista、Windows Server 2008 及以上版本操作系统。在 Windows XP 系统中，任何版本的 IE 浏览器都不支持 SNI。）
- Konqueror 4.7 及以上版本
- Opera 8 及以上版本
- Safari 3.0 及以上版本（仅支持 Windows Vista、Windows Server 2008 及以上版本操作系统，或 Mac OS X 10.5.6 及以上版本操作系统。）

SNI 支持以下客户端-手机端浏览器：

- Android 3.0 Honeycomb 及以上版本
- iOS 4 及以上版本
- Windows Phone 7 及以上版本

SNI 支持以下服务器：

- Apache 2.2.12 及以上版本
- Apache Traffic Server 3.2.0 及以上版本
- Cherokee
- HAProxy 1.5 及以上版本
- IIS 8.0 及以上版本
- Lighttpd 1.4.24 及以上版本

- LiteSpeed 4.1 及以上版本
- Nginx 0.5.32 及以上版本

SNI 支持以下命令行：

- cURL 7.18.1 及以上版本
- wget 1.14 及以上版本

SNI 支持以下库：

- GNU TLS
- JSSE (Oracle Java) 7 及以上版本（仅作为客户端）
- libcurl 7.18.1 及以上版本
- NSS 3.1.1 及以上版本
- OpenSSL 0.9.8j 及以上版本
- OpenSSL 0.9.8f 及以上版本（需配置 flag）
- Qt 4.8 及以上版本

7.11 HTTPS证书转换成PEM格式

PEM 格式的证书文件（*.pem）一般为以下格式：

说明：

PEM 格式证书文件可用 notepad++ 等文本编辑器打开。

```
-----BEGIN CERTIFICATE-----
62EcYPWd2Oy1vs6MTXcJSfN9Z7rZ9fmxWr2BFN2XbahgnsSXM48ixZJ4k
rc+1M+j 2kcubVpsE2cgHdj4v8H6jUz9Ji4mr7vMNS6dXv8PUkl/qoDeNG
CNdyTS5NIL5ir+ g92cL8IGOkjgvhlqt9vc65Cgb4mL+n5+DV9uOyTZT
W/MojmlgfUekC2xiXa54nxJ f17Y1TADGSbyJbsC0Q9nIrHsPl8YKkvRWvI
AqYxXZ7wRwWWmv4TMxFhWRiNY7yZI o2ZUhl02SIDNggIEeg==
-----END CERTIFICATE-----
```

对于 CER / CRT 格式的证书，您可通过直接修改证书文件扩展名的方式进行转换。例如，将“server.crt”证书文件直接重命名为“server.pem”即可。

PFX 格式证书转换为 PEM 格式

PFX 格式的证书一般出现在 Windows Server 服务器中，您可通过 openssl 工具进行转换。

例如，通过执行以下两条 openssl 命令即可把 certname.pfx 证书转换成 PEM 格式。

- 提取私钥命令：`openssl pkcs12 -in certname.pfx -nocerts -out key.pem -nodes`

- 提取证书命令：`openssl pkcs12 -in certname.pfx -nokeys -out cert.pem`

P7B 格式证书转换为 PEM 格式

P7B 格式证书一般出现在 Windows Server 和 Tomcat 服务器中，您可通过 openssl 工具进行转换。

转换步骤

参照以下步骤，将 P7B 格式证书转化为 PEM 格式。

1. 证书转换。例如，执行 `openssl pkcs7 -print_certs -in incertificat.p7b -out outcertificate.cer` 命令将 *incertificat.p7b* 证书文件转换成 *outcertificate.cer* 格式。
2. 获取*outcertificat.cer* 文件中`[-----BEGIN CERTIFICATE-----`与`-----END CERTIFICATE-----]`中的证书内容。
3. 将证书内容保存为 PEM 格式即可。

DER 格式证书转换为 PEM 格式

DER 格式的证书一般出现在 Java 平台中，您可使用 openssl 工具将其转化为 PEM 格式。

例如，通过执行以下两条 openssl 命令可以把 *certificate.cer* 证书转换成 PEM 格式。

- 提取证书：`openssl x509 -inform der -in certificate.cer -out certificate.pem`
- 提取私钥：`openssl rsa -inform DER -outform PEM -in privatekey.der -out privatekey.pem`

更多关于证书格式的问题，请参考 主流数字证书都有哪些格式?

7.12 HTTPS业务异常状态说明

错误日志内容	详情	备注
证书私钥不匹配	上传的证书和私钥不匹配	无
证书格式不对	证书不符合标准格式	无

7.13 香港高防备用IP使用说明

香港备用IP的主要作用是给用户用于在主机房故障的时候切换使用，平时用户只需要把配置配上即可，切勿切业务流量到备用IP上。

建议使用场景：

- 配置备用IP并测试。
- 平常主要使用主IP，当主IP机房故障的时候，可以把业务切换到备用IP上，平时切勿切换。

7.14 访问高防端口不通排查

本文档适用于端口访问一直不通的场景。

说明：

如果您的三线高防网络链路（BGP、电信和联通）同时出现问题，请参考高防IP卡顿、延迟、访问不通等问题排查。

针对单一运营商（比如电信）或单一地域（比如兰州），用户在访问对应的高防节点时无法访问，但访问另外一个节点就正常了。

问题分析

遇到此类问题时，需要收集基础信息，首先确认问题影响范围，然后获取全面的诊断信息，进行分析定位和相应处理。

排查思路

参照以下步骤进行排查。

1. 确保没有跨运营商访问。
2. 获取以下基础信息：客户端IP、运营商信息、无法访问的端口。
3. 获取以下全面诊断信息：
   - ping 测试结果截图
   - 端口 telnet 测试结果截图
   - 具体的报错信息全屏截图
   - 端口路由跟踪，进行端口可用性探测

     具体请参考端口可用性探测说明。
   - 无法 ping 时，通过 tracert 或 mtr 等工具进行链路测试

     具体请参考链路测试说明。

   如果结和以上信息，仍没有定位出问题，您需要在服务端以及客户端进行抓包分析。

   具体请参考抓包操作说明。
4. 根据上述信息定位出问题后，联系相关部门进行处理。

案例分享

问题描述

接到某高防用户反馈，A省x市电信用户，在访问高防节点的80端口时出现异常，但是访问443端口是正常的。

分析步骤

1. 分析/获取以下基础信息：
   - A省的x市电信用户 高防节点80端口：问题范围明确。
   - 访问443端口是正常的：说明整个链路是通的，只是个别端口有问题。
   - 联系最终用户，获取具体的IP地址是：x.x.x.x
   - 联系最终用户，获取 ping\telnet\ 报错的结果。
   - 联系最终用户，获取端口跟踪正常与不正常的结果对比。
2. 定位问题。根据上述最后一条信息，端口跟踪路由在x市的网络出口处中断。
3. 问题处理。联系运营商处理。由于客户端市级运营商安全策略调整导致问题，调整后恢复。

7.15 高防IP是否需要网站备案接入

高防 IP 分为电信线路、联通线路、BGP 线路和香港线路。

- 电信和联通线路只需要在工信部备案，不需要在阿里云备案。即有备案号即可使用高防 IP 服务。
- BGP 线路需要在阿里云接入备案。
- 香港线路面向源站在香港及东南亚地区的用户，不需要 ICP 备案或阿里云备案。

> 说明:
> 如果源站在大陆地区，仍需按照工信部要求进行 ICP 备案，未备案域名将依照相关法律法规进行查封。

关于如何进行备案，请参考 阿里云备案。

> 说明:
> 源站在中国大陆地区的网站不建议使用香港高防防护，推荐使用大陆地区的高防线路，并依照相关备案流程进行接入。

7.16 上传HTTPS证书出现“参数错误”解决办法

在配置高防 IP 服务过程中，上传 HTTPS 证书时，提示“参数格式错误”。

在上传证书时出现“参数错误”的常见原因和解决方法如下：

- 证书名字过长。

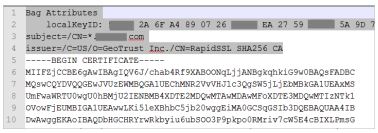
  解决方法：修改证书文件名为 10 个字符以内。

- 证书文件名中包含特殊字符。

  解决方法：仅以英文字符或数字命名证书，不要包含空格、下划线、分隔符等特殊字符。

- 证书内容中存在不规范的内容。

  示例



  解决方法

  删除证书文件中`---BEGIN CERTIFICATE---`之前的内容。

  - 规范的证书（.pem 文件）内容示例：

  - 规范的私钥（.key 文件）内容示例：

关于 HTTPS 证书的格式转换的信息，请参考*HTTPS证书转换成pem格式*。

7.17 配置高防后业务访问报502错误

概述

本文主要介绍配置高防后业务访问报502错误的排查思路。

详细信息

1. 通过本地Hosts解析，直接解析到后端SLB地址，尝试访问查看是否有异常，如果仍旧出现502报错，需要核实负载均衡SLB相关配置 。
2. 核实负载均衡健康检查是否有异常。
3. 如果直接解析到SLB访问正常，需要核实高防配置是否异常 。

说明:

- 充分了解高防以及SLB的具体配置。
- 熟悉SLB的健康检查配置。
- 熟悉高防回源的基本原理。

适用于

- 云安全防御

7.18 高防告警短信配置

概述

本文主要介绍高防告警短信配置的方法。

问题描述

无法收到提示信息。

解决方案

1. 登录阿里云控制台,单击页面右上方控制台， 进入管理控制台后，单击页面上方 消息 进入 消息中心，再单击左侧导航栏中 基本接收管理。
2. 选择 消息接收管理，修改 产品的释放信息通知和云盾（安全）产品信息通知中的联系人。

适用于

- 云安全防御

7.19 配置高防后访问业务缓慢

概述

本文主要介绍配置高防后访问业务缓慢的解决方法。

问题描述

服务器配置高防后，业务访问时间从原来的1秒变成8秒，业务访问缓慢。

解决方案

1. 通过Chrome浏览器访问业务，使用Chrome浏览器开发者工具进行观察，访问业务在等待了7-10秒后，开始加载业务的其他资源。
2. 基于高防IP地址进行抓包分析，发现业务在连接8000端口之前，一直在尝试连接843端口，消耗的时间大约在8秒左右。

    说明:
   业务程序需要使用到843和8000端口，没有配置843端口转发，导致连接缓慢。
3. 业务 控制台在配置843端口的转发后，业务访问恢复正常。

适用于

- 云安全防御

7.20 配置高防后通过http和https上传大文件失败

概述

本文主要介绍配置高防后通过http和https上传大文件失败的解决方法。

问题描述

经过高防后上传4.8GB的文件进度一直停止不动，上传失败。

问题原因

高防配置的最大上传文件大小为300M，后端nginx也有配置最大上传文件大小。

解决方案

1. 压缩文件上传，让上传文件小于300M 。
2. 大文件建议放OSS等存储上。
3. 跳过高防，绑定HOST直接访问ECS进行测试。

适用于

- 云安全防御

7.21 如何跨账户配置高防

概述

本文主要介绍如何跨账户配置高防。

详细信息

1. 多个账户（实名认证账户）同时提交问题工单，说明相同需求： 希望共用某个账号下的高防IP地址。
2. 系统审核通过后，将高防IP账号的UID与其他账号的UID进行关联，处理完成后，可以直接在另外一个帐号下配置高防IP。

适用于

- 云安全防御

7.22 配置高防后系统建立连接慢

问题描述

配置高防后系统建立连接慢。

问题原因

Windows Server 2012 引入的新功能ECN(Explicit Congestion Notification)导致。

解决方案

1. 登录ECS服务器。
2. 以管理员身份运行CMD，执行如下命令，关闭系统ECN功能。

```
netsh int tcp set global ecncapability=disabled
```

系统显示类似如下，表示ECN已经关闭。

说明:

ECN功能是根据RFC规定来减少网络包重传的机器，但是由于中国大陆地域的某些ISP封杀此类的SYN包，导致目标机器无法收到带有ECN标志的SYN包，Windows机器在发送2次ECN包没有得到响应后(第一次重传3秒，第二次重传6秒)，会采用没有ECN标志位的SYN包，后续可以连接成功。

适用于

- 云安全防御

7.23 GET请求返回的HTTP状态为413错误

概述

本文主要介绍GET请求返回HTTP状态为413错误的排查步骤。

问题描述

GET请求头大小超过10k时，返回的HTTP状态为413错误。

解决方案

1. 架构为高防-->WAF-->SLB-->ECS，通过浏览器调试模式查看返回的HTTP状态为413。
2. 如果SLB是TCP模式监听，说明是Nginx的client_max_body_size配置过小的问题。
3. 使用本地Hosts解析到ECS实例测试，同样返回的HTTP状态为413，确认是Nginx配置问题导致的。

更多信息

相应产品的client_max_body_size配置限定值如下。

- 高防 800M
- WAF 3M
- SLB 50G

适用于

- DDoS高防IP

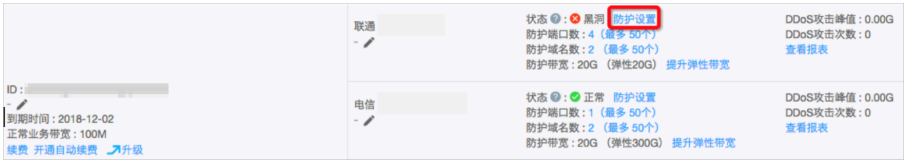
7.24 配置高防IP后无法Ping通

概述

本文主要介绍配置高防IP后无法Ping通的解决方法。

详细信息

1. 确认配置高防IP的状态是否处于黑洞状态，黑洞状态无法被外网访问。



2. 确认购买高防IP后是否启用且正常配置，未配置任何的网站接入以及非网站接入，也会无法ping通。
3. 如果 根据常规的网络测试方法进行排查还是无法Ping通，获取Ping/MTR等日志信息，提交阿里云技术支持解决。

适用于

- 云安全防御

7.25 NTP服务的DDoS攻击

概述

NTP协议(network time protocol)是标准的网络时间同步协议，它采用层次化时间分布模型。网络体系结构主要包括主时间服务器、从时间服务器和客户机，主时间服务器位于根节点，负责与高精度时间源进行同步，为其他节点提供时间服务，各客户端由从时间服务器经主服务器获得时间同步。

详细信息

NTP服务的DDoS攻击原理

NTP协议是基于UDP协议的服务器/客户端模型，由于UDP协议的无连接性(不像TCP具有三次握手过程)具有天然的不安全性缺陷，黑客正是利用NTP服务器的不安全性漏洞发起DDoS攻击。

1. 寻找目标，包括攻击对象和网络上的NTP服务器资源。
2. 伪造要“攻击对象”的IP地址向NTP服务器发送请求时钟同步请求报文，为了增加攻击强度，发送的请求报文为monlist请求报文。NTP协议包含一个monlist功能，用于监控 NTP 服务器，NTP 服务器响应monlist指令后就会返回与其进行过时间同步的最近 600 个客户端的IP地址，响应包按照每6个IP进行分割，最多一个NTP monlist请求会形成100 个响应包，具有较强的放大能力。实验室模拟测试显示，当请求包的大小为234字节时，每个响应包为 482 字节，单纯按照这个数据,计算出放大的倍数是：482*100/234 = 206倍，从而大流量阻塞网络，导致网络不通，无法提供服务。

NTP服务的DDoS防御原理

1. 购买足够大的带宽，硬性抵挡NTP服务的DDoS攻击产生的大流量攻击。
2. 使用DDoS防御产品，将入口异常流量进行清洗，正常流量和区分异常，将正常流量分发给服务器进行业务处理。
3. 通过防火墙对UDP使用的123端口进行限制，只允许NTP服务与固定IP进行通信，其他IP全部拒绝。
4. 关闭NTP服务器monlist功能。
5. 升级NTP服务器版本到4.2.7p26。

适用于

· DDoS高防IP

7.26 配置高防后不能实现会话保持的排查思路

概述

本文主要介绍配置高防后不能实现会话保持的排查思路。

问题描述

业务配置高防后，域名接入后进行测试，登录后单击任意的菜单，将会退出登录。

问题原因

1. 没有开启会话保持。

2. 请求经过高防后，高防默认会在Cookie中加入一串高防防攻击用的字段，增长了网站本身的Cookie长度，如果源站服务处理不妥当会出现问题。

```
http_cookie:  aliyungf_tc=AQAAAFvyfRtP/AIATUWYDheCsQtZUPVB; SSID=
19mjjcefouv7f8cpbuhp2f9lv2; current_menu=%2F
```

3. 判断用户Session的存储有基于源IP的校验。高防/WAF开启会话保持是指开启高防IP的LVS到高防IP的Tengine这一段，对于SLB后端的服务器而言，同一个客户端的请求，SLB看到的客户端IP只有一个，即会话保持的那个Tengine的IP地址。 如果不开启会话保持，则对SLB的后端的服务器而言，同一个请求，看到的会有多个客户端IP(Tengine)。

解决方案

1. 开启TCP监听的会话保持。
2. 调整监听为HTTP模式，开启会话保持。
3. 在 配置高防之前，直接访问源站SLB，且没有开启会话保持，访问是正常的。说明登录会话保持，不是依赖SLB实现的。
4. 会话保持的实现方式是使用Session的方式实现的，同时Session全部保存在MemCache中。Session的信息存放在客户端的Cookies中，获取时是通过Session的ID获取，取SSID值，而非依据顺序获取。
5. 开启高防IP的会话保持。

适用于

- DDoS高防IP

7.27 如何判断DDoS高防IP的攻击类型

概述

当DDoS高防IP同时受到CC类型和DDoS类型攻击时，需快速判断攻击类型，进行对应的处理。

详细信息

判断思路

1. 两种攻击类型的特点：
   - CC类型攻击作用于7层网站连接数。
   - DDoS类型攻击作用于4层流量。
2. 查看用户受到攻击的情况。
   - 如果只配置了4层转发，一般攻击是DDoS的。控制台登录查看对应防护流量信息， DDoS防护有攻击流量的波动，且在清洗，在CC防护中没有相关的波动。

- 如果只配置了7层转发，一般攻击是CC攻击。控制台登录查看对应防护流量信息，DDoS防护有攻击流量的波动，且在清洗，在 CC防护中有相关的波动。

> 说明:
> 由于DDoS防护是4层的信息，而CC攻击是7层的攻击，在流量异常后DDoS会进入清洗状态，但是无法有效的清洗掉CC攻击，最终会在CC防护处看到真正的CC清洗效果。

控制台监控说明

流量的经过顺序如下：流量 > DDoS防护 > CC防护

如果这2个防护都没有拦截攻击，那么攻击将会到达源站。

适用于

- DDoS高防IP

7.28 HTTP报文经过Web应用防火墙后响应头没有Content-Length

概述

本文主要介绍HTTP报文经过Web防火墙后，响应头没有Content-Length的处理方法。

问题原因

Web应用防火墙 开启了防敏感信息。

解决方案

Web应用防火墙中防敏感信息泄漏会修改响应头，所以会清掉Content-Length，可以先把防敏感信息泄漏关闭掉。

适用于

- Web应用防火墙

7.29 网站防护和非网站防护的区别

网站防护

网站防护针对 HTTP/HTTPS 协议，仅支持 80 和 443 端口，提供针对三层到七层的DDoS攻击防护，可防护包括SYN flood、ACK flood、UDP flood、ICMP flood、CC（HTTP flood）等攻击。

非网站防护

非网站防护针对四层的TCP和UDP协议，不支持 80 端口和 UDP 53 端口（如您需要 DNS 防护服务，请使用云解析产品），提供针对三层到四层的各类DDoS攻击防护，可防护包括SYN flood、ACK flood、UDP flood、ICMP flood等攻击，但无法防护基于七层的攻击，如HTTP flood攻击。支持针对目的IP和端口级别的TCP连接层面的新建，并发等限速控制。

本质区别

非网站防护（四层防护）无法解析到七层的报文内容，因此无法针对七层的内容做防护策略。

说明:

对于特殊类型的 Web 类业务（如 Web socket）和非标端口的的 Web 业务（如8080、8888、4433等），可以使用四层转发配置 DDoS 高防 IP 服务。

7.30 健康检查主动探测IP

DDoS高防IP服务使用特定的IP主动探测所防护的源站服务器的健康状态，建议您放行这些健康检查的主动探测IP。

为了确保源站服务器可以正常处理经DDoS高防IP服务转发的正常业务流量，高防IP将不定期的对所接入防护的源站服务器进行主动探测，实现健康检查。

DDoS高防IP服务使用固定的IP对您的源站服务器进行主动探测，其探测行为仅为确认源站服务器的健康状态，对您的源站服务器不会产生任何影响。如果在源站服务器的访问日志中发现来自主动探测IP的数据包，您不必担心源站是否已遭受恶意攻击。同时，为确保DDoS高防IP服务的健康检查功能正常工作，建议您在源站服务器的访问控制策略中将这些健康检查主动探测IP加入白名单。

网络三层（Ping）主动探测IP

地域	主动探测IP
华北1（青岛）	47.104.162.123
华北2（北京）	39.107.84.97
华东1（杭州）	47.97.187.10
华东2（上海）	47.100.176.74
华南1（深圳）	120.78.69.183
大连联通cn335线路	211.93.148.207
香港	47.52.224.185
新加坡	47.74.135.107
澳大利亚（悉尼）	47.91.45.70
马来西亚（吉隆坡）	47.254.197.21
美国（弗尼吉亚）	47.90.210.37
美国（硅谷）	47.254.31.65
德国（法兰克福）	47.254.133.240

网络四层和七层主动探测IP

类型	主动探测IP
私网	· 10.181.0.186 · 10.181.0.187 · 10.181.2.120 · 10.181.2.126
公网	· 140.205.205.7 · 140.205.205.6 · 140.205.205.15 · 140.205.205.11

附录：探测行为数据包示例