ALIBABA CLOUD

阿里云

DDoS防护
DDoS高防（旧版）

文档版本：20211103

阿里云

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
危险	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。	危险 重置操作将丢失用户配置数据。
警告	该类警示信息可能会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，恢复业务时间约十分钟。
注意	用于警示信息、补充说明等，是用户必须了解的内容。	注意 权重设置为0，该服务器不会再接受新请求。
说明	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。	单击**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。	在**结果确认**页面，单击**确定**。
Courier字体	命令或代码。	执行 `cd /d C:/window` 命令，进入Windows系统文件夹。
斜体	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。	`switch {active|stand}`

目录

1.从高防IP迁移至新BGP高防IP

本文介绍了从阿里云静态高防IP将被防护业务迁移到新BGP高防IP的相关内容。

背景信息

距离阿里云静态高防IP服务机房上线已经过了三年时间，随着用户业务对链路稳定性要求的提升，这三年间我们一直致力于改善我们的高防IP产品。

在此，我们很高兴地通知您，阿里云目前已可以为您提供支持八线BGP网络的高防IP服务：新BGP高防IP。

新BGP高防IP重构了底层网络，新BGP高防IP服务的网络架构与阿里云BGP线路机房互通，彻底解决以往单线电信、单线联通网络中存在的跨网访问质量问题，实现全国各地与新BGP高防IP的平均延迟在20 ms以内。同时，在新BGP高防IP架构中，每个运营商遭受的攻击流量都将在对应运营商的网内解决，使得新BGP高防IP服务在网络层灾备和攻击防护能力方面都有质的提升。

新BGP高防IP规格说明

- 基础防护能力：最低支持30 Gbps保底防护带宽（月单价20,800元起）
- 弹性防护能力：与您当前高防IP实例的弹性防护带宽一致，最高支持600 Gbps弹性防护带宽（超过600 Gbps以上的防护能力需求可联系我们定制）

迁移至新BGP高防IP

为了让您能享受新BGP高防IP稳定、快速、安全的服务，现诚邀您将在用的静态机房的高防业务迁移至新BGP高防IP，立即体验稳定和快速的新BGP高防IP服务。

您可以在现有高防服务到期前，购买新BGP高防IP服务，将原静态机房的高防业务平滑地迁移至新BGP高防IP服务。

> **说明** 建议您在获得新BGP高防IP实例后尽快完成新BGP高防IP实例的配置。迁移过程中，您的待迁移高防IP实例将与新BGP高防IP实例共存，且都可以正常转发业务流量。

开始之前

强烈建议您在正式开始迁移前，在云盾DDoS高防IP管理控制台中使用域名配置、转发规则批量导出功能，将当前的网站和非网站业务接入配置导出备份。在您将域名配置迁移至新BGP高防IP实例后，原高防IP实例中将无法查看到原有域名配置信息。

注意事项

- 整个业务配置迁移同步过程中将不会对您的业务造成任何影响。如果您需要回滚业务配置，请提交工单或通过钉钉服务群的方式联系我们进行操作。
- 在原高防IP实例与新BGP高防IP实例共存期间和迁移过程中，为避免产生不必要的弹性后付费，建议您将原高防IP实例的弹性防护带宽设置为与保底防护带宽一致。

操作步骤

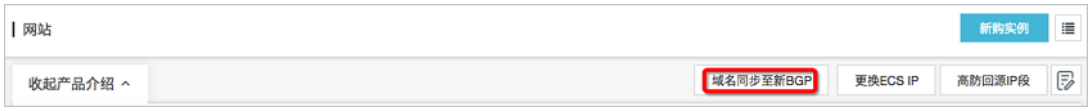
1. 登录云盾DDoS高防IP管理控制台。
2. 将业务配置迁移至新BGP高防IP实例。
   - 网站域名配置迁移

     域名配置迁移前注意事项：

     - 请勿在新BGP高防IP实例中添加80或443的端口转发配置。因为新BGP高防IP的域名配置默认占用80或443端口进行转发，如果在新BGP高防IP实例中已添加80或443端口配置，将导致所迁移的域名配置无法正常关联新BGP高防IP实例。

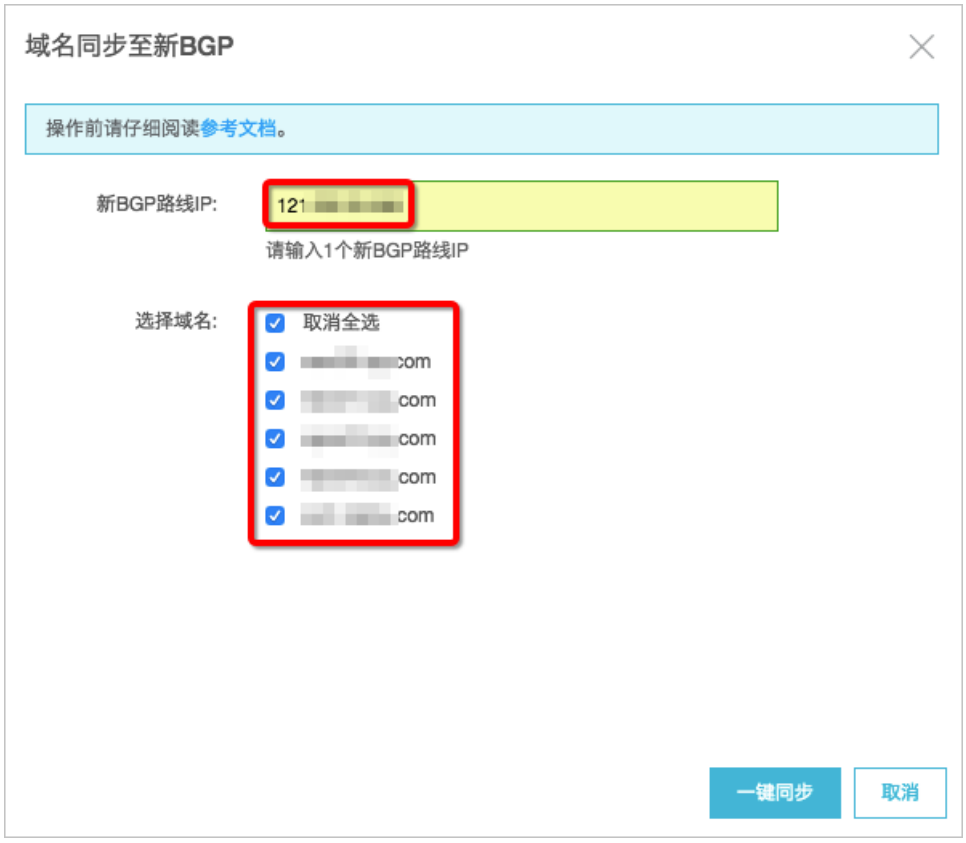
- 如果您之前通过提交工单在后台开通HTTP2或HTTPS强制转HTTP回源的功能，请务必在域名同步前关闭这些功能。
- 当所迁移的域名与其它账号的泛域名配置存在冲突时，将导致所迁移的域名配置无法正常关联新BGP高防IP实例。如果您拥有多个阿里云账号，请注意检查是否存在此类冲突。

a. 定位到**接入 > 网站**，单击**域名同步至新BGP**。



b. 输入阿里云为您创建的新BGP高防IP实例的IP，选择所需迁移的域名配置。

> **说明** 一次最多支持选择五个域名。如果原高防IP实例中包含超过五个需要迁移的域名配置，请分多次进行域名同步。



c. 单击**一键同步**，并确认，将所选择的域名配置迁移至新BGP高防IP实例。您可以在新BGP高防IP管理控制台的**接入管理 > 域名接入**页面中查看已迁移的域名配置信息。

> **说明** 此时，您的网站业务流量依然由原高防IP实例转发，对您的业务防护不会产生任何影响。

域名同步操作注意事项：

- 如果所需迁移的域名配置仅关联一个高防IP实例，您只需按上述步骤将所有域名配置同步至新BGP高防IP即可。
- 如果您拥有多个高防IP实例，且部分域名关联多个高防IP实例，则必须先明确所需迁移的域名及这些域名当前已关联的高防IP实例情况。如果其中存在部分高防IP实例将继续使用且短期内不会释放，建议您先将所需迁移的域名与这些高防IP实例解除关联，再按上述步骤进行迁移。

> **注意** 域名同步完成后，您在云盾DDoS高防IP管理控制台中将无法看到已迁移的域名配置，但实际上这些域名与原高防IP实例的关联关系依然存在且生效，而原高防IP实例中显示的已关联域名数量不会变化。您可以在新BGP高防IP管理控制台的**接入管理 > 域名接入**页面中查看已迁移的域名配置信息。因此，为了避免在云盾DDoS高防IP管理控制台中对已迁移的域名配置进行错误变更，因此在云盾DDoS高防IP管理控制台中隐藏这些域名配置记录。

d. 域名同步完成后，建议您将在新BGP高防IP管理控制台的**接入管理 > 域名接入**页面中查看到的已迁移的域名配置与迁移前导出的域名配置信息进行比对。如果发现迁移后的配置存在差异，您需要在新BGP高防IP管理控制台中按照原配置信息手动更改域名配置。

域名配置迁移后注意事项：

- 新BGP高防IP使用的回源网段与高防IP不同，如果您的源站对访问IP存在限制，请在**接入管理 > 域名接入**页面中单击**查看回源IP网段**，并将所有网段地址添加至源站访问控制策略的白名单中。
- 如果您的域名尚未通过阿里云备案，您可以提交工单或通过钉钉服务群联系我们申请暂时放行。强烈建议您尽快为该域名完成阿里云备案。

- 非网站业务配置迁移

a. 定位到**接入 > 非网站**，选择所需迁移的高防IP实例和高防IP。

b. 单击**导出规则/配置**，选择**导出规则**。

c. 在新BGP高防IP管理控制台的**接入管理 > 端口接入**页面，选择实例，单击**批量操作**，选择**添加规则**。

d. 将从原高防IP实例中导出的规则配置信息粘贴至文本框中，单击**添加**，即可将端口转发规则配置迁移至新BGP高防IP实例。

> **说明** 在完成端口配置迁移后，您也可以通过批量操作的方式将原高防IP实例中非网站业务的会话保持、健康检查配置或DDoS防护策略配置迁移至新BGP高防IP。

3. 参见本地验证配置，通过本地修改Host文件的方式绑定新BGP高防IP实例的IP，逐条检查网站和非网站配置是否生效。
4. 验证通过后，前往您域名对应的DNS服务商提供的域名解析管理页面，修改域名DNS解析设置，通过**A记录**的方式，将域名解析指向新BGP高防IP实例。

> **说明** 如果您的非网站业务未使用域名进行连接，将您业务IP替换为所配置的新BGP高防IP实例的IP，即可正式将业务流量切换至新BGP高防IP实例。

5. 确认所有业务均已迁移至新BGP高防IP实例后，如果您的原高防IP实例仍在服务期内，您可以提交工单申请退回原高防IP实例的余款；如果您的原高防实例IP实例已经到期，建议您及时释放原高防IP实例。

> **说明** 原高防IP实例与新BGP高防IP实例共存期间，您无法在新BGP高防IP管理控制台中删除所迁移的网站域名配置。只有在该域名所关联的原高防IP实例释放后，才可删除该域名配置。

常见问题

- 新BGP高防IP产品有哪些优势？

  关于新BGP高防IP的优势，请参见什么是新BGP高防IP。

- 新BGP高防IP产品的价格明细？

  关于新BGP高防IP产品的产品定价，请参见新BGP高防IP计费方式。

- 新BGP高防IP产品的链路质量如何？

  您可以通过以下第三方测试工具测试新BGP高防IP产品的线路延迟情况：
  http://ping.chinaz.com/203.107.32.57

  测试IP：203.107.32.57

- 业务迁移至新BGP高防IP大约需要多久？
  - 网站类业务：通常由于DNS刷新等原因，需要1~3天左右完成。
  - IP类业务：需要根据您的业务实际情况进行评估。

- 业务迁移会导致业务中断吗？

  一般情况下，迁移至新BGP高防IP实例的过程中不会对您的业务产生影响，但具体情况仍需要您根据实际业务进行评估。阿里云保证您的新BGP高防IP实例与原有高防IP实例将共存一段时间，当您将全部业务流量都迁移至新BGP高防IP实例后，阿里云将再次确认业务流量已经全部迁移完成后，才会释放原有的高防IP实例。

  整个迁移过程中，阿里云都将以保障您的业务访问作为第一优先级。

- 迁移至新BGP高防IP还有哪些注意事项？
  - 新BGP高防IP实例使用的是BGP线路的IP，天然具备故障发生时的自动切换线路能力（且相比通过DNS解析切换更快、更稳定）。
  - 新BGP高防IP实例的回源IP段信息与原高防IP实例不同。如果您在高防IP实例后端配置了回源IP地址限制等策略，您需要手动更新回源IP段信息。

2.产品简介

2.1. 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。

购买DDoS高防IP服务后，您需要把域名解析到高防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。配置完成后，所有公网流量都将经过高防IP机房，在机房清洗过滤恶意攻击流量，然后将正常流量通过端口协议转发的方式转发到源站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。

> **注意** 目前，旧版DDoS高防IP服务已停止售卖。如果您有DDoS攻击防护需求，请选购新版DDoS高防服务。详细信息，请参见什么是DDoS高防（新BGP&国际）。

2.2. 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。

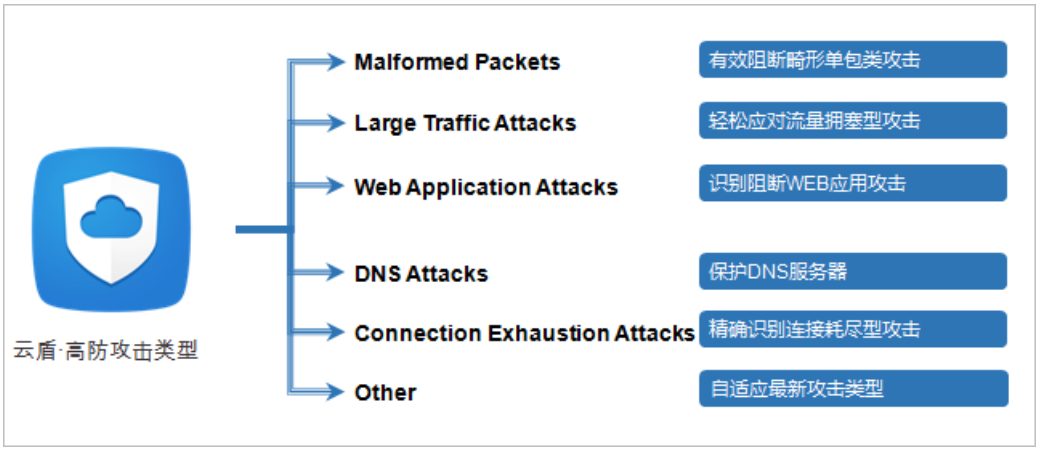
阿里云云盾产品所涉及的产品组件，全部为自主研发产品，拥有充分自主知识产权。

从引流技术上，DDoS高防IP服务支持BGP与DNS两种方案；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。

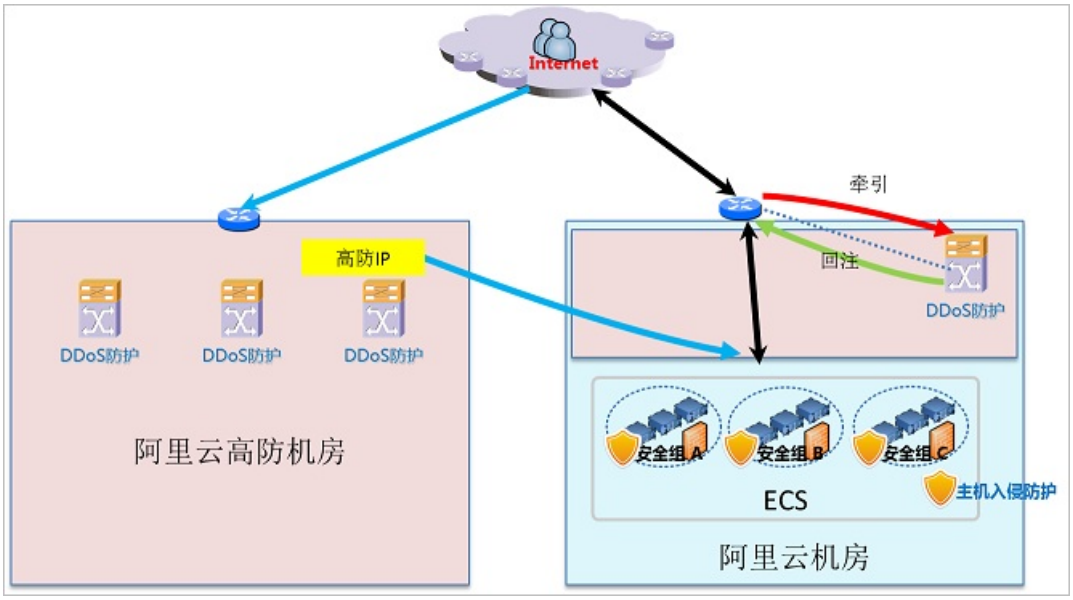
针对攻击，阿里云在传统的代理、探测、反弹、认证、黑白名单、报文合规等标准技术的基础上，结合Web安全过滤、信誉、七层应用分析、用户行为分析、特征学习、防护对抗等多种技术，对威胁进行阻断过滤，保证被防护用户在攻击持续状态下，仍可对外提供业务服务。

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见下图。

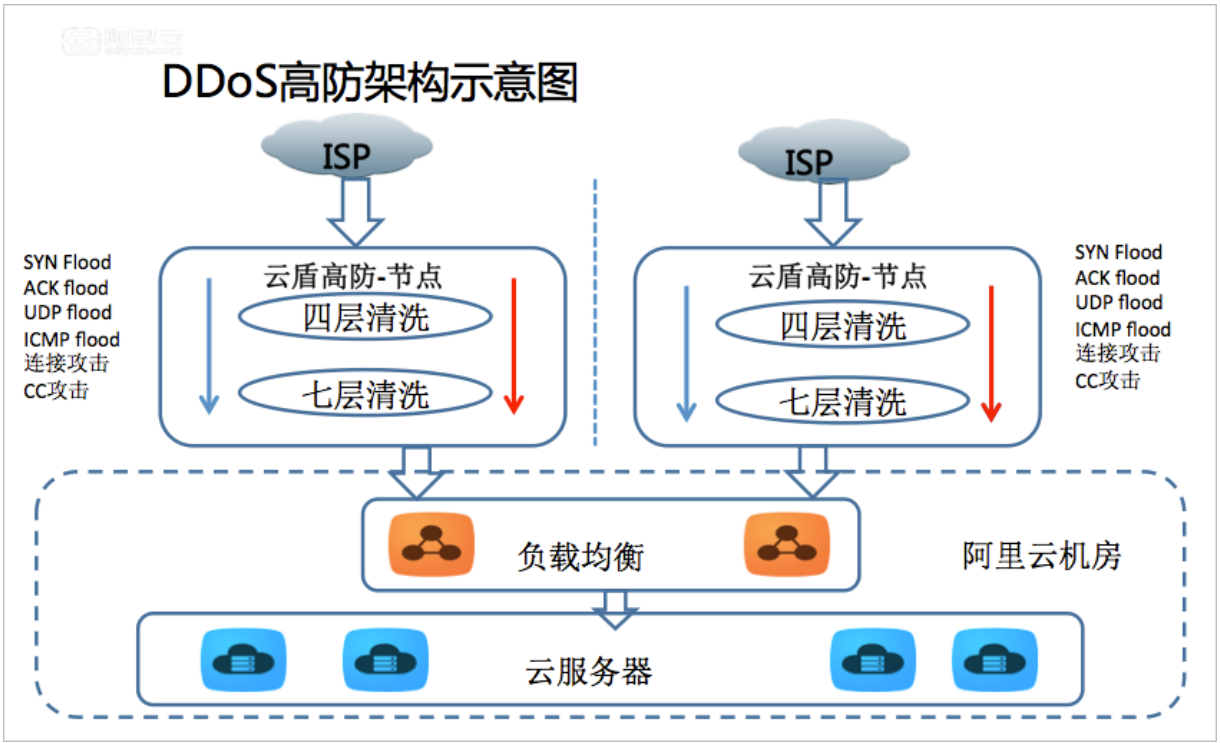


DDoS高防IP服务使用专门的高防机房为您提供DDoS防护服务。网络拓扑示意图如下。



在上图中，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。



2.3. 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。
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。

2.4. 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。

3.产品定价

3.1. 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。

前提条件

购买高防IP服务前，您需完成实名认证。

背景信息

> **说明** 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。

  > **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实例的最大弹性防护带宽。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大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

3.2. 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，保底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：保底防护 + 弹性防护

付费方式：预付费 + 后付费

计费周期：保底防护带宽（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，防御能力下调到保底防护带宽能力。

- 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：您可以选择升级保底防护的防护能力。

  例如，您可以从 20Gbps/60,000QPS 升级到 300 Gbps/1,000,000QPS 的保底防护能力。

> **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。

3.3. 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。

3.4. 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。

3.5. 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。

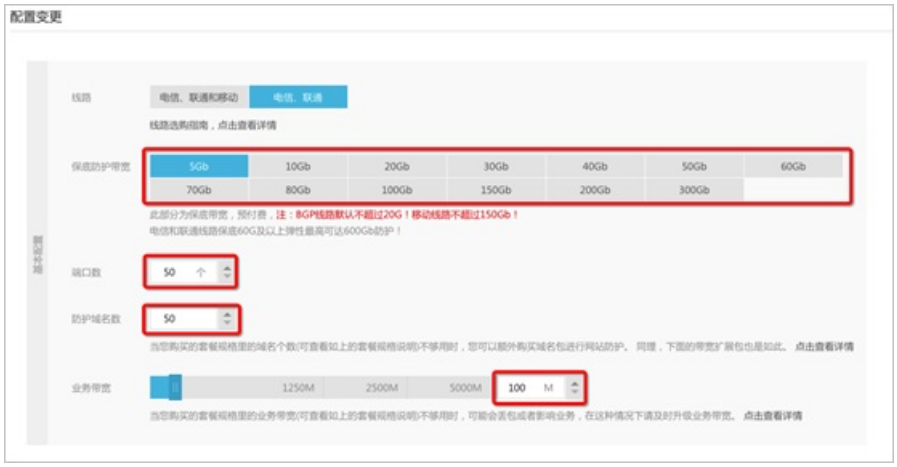
  > **说明** 该高防IP实例的业务带宽超过 550 M 后，每增加 1 M 按 75 元/月的单价计算差价。

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。

3.6. 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

4.快速入门

4.1. 防护网站业务

4.1.1. 概述

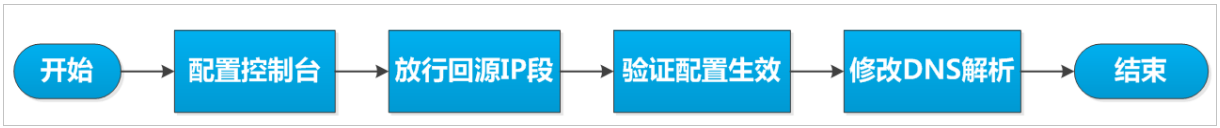
本文档介绍了网站业务用户新购DDoS高防后如何配置上线、切换业务接入高防、并验证防护生效。

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。

4.1.2. 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高防管理控制台。
2. 定位到**资产 > 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**。

后续步骤

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。

4.1.3. 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，高防将自动匹配该泛域名对应的子域名。例如，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。
> - 如果同时存在泛域名和精确域名配置（如 *.aliyun.com 和 www.aliyun.com ），WAF优先使用精确域名所配置的转发规则和防护策略。
> - 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。

4.1.4. （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**选项同时选中**http**和**https**。

   > **注意** 网站只有HTTPS业务（没有HTTP业务）的情况，也需要选中**http**协议类型。

   选中**https**协议类型后，您会收到以下提示信息：**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。
3. 单击**确定**，完成域名转发规则的配置。
4. 在域名列表，定位到刚添加的域名，单击**业务状态**列下**https**后的**上传**。

5. 复制证书和私钥文本内容，完成证书上传。

   PEM、CER或CRT证书格式可用文本编辑器直接打开进行复制。其他特殊格式（例如，PFX、P7B等）的证书需要先转换成PEM格式。

   相关操作，请参见高防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。

   证书格式示例：

```
-----BEGIN CERTIFICATE-----
……
-----END CERTIFICATE-----
```

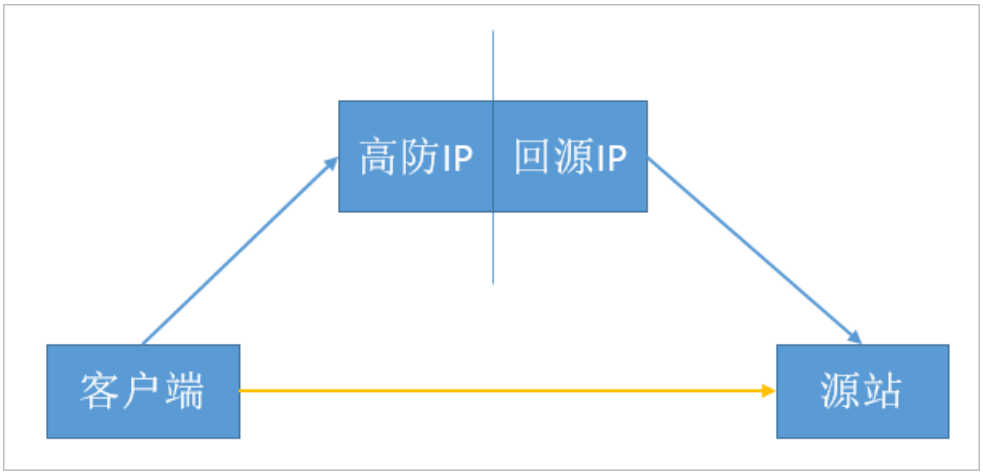
私钥格式示例：

```
-----BEGIN RSA PRIVATE KEY-----
……
-----END RSA PRIVATE KEY-----
```

6. 单击**确定**。
   证书上传完毕后，HTTPS业务状态显示为正常。

4.1.5. 步骤2：放行回源IP段

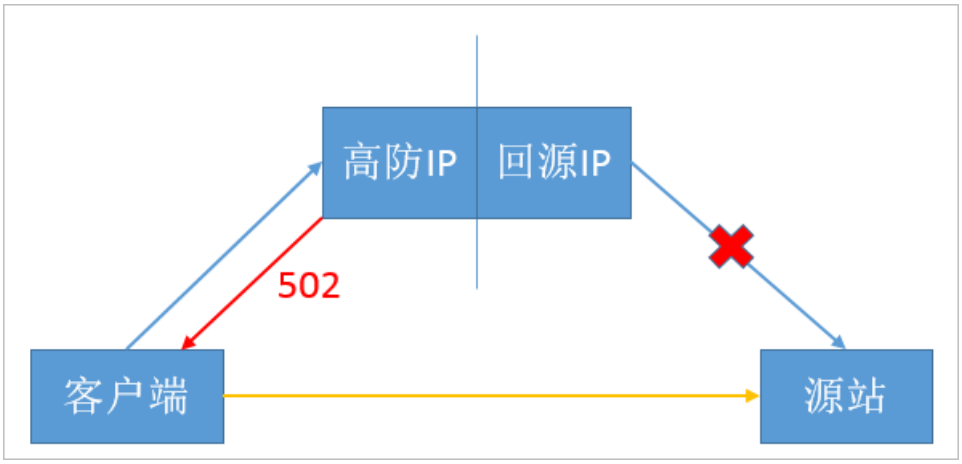
DDoS高防作为一个反向代理，其中包含了一个Full NAT的架构。



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。

4.1.6. 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：
   i. 找到Hosts文件。一般Hosts文件在 C:\Windows\System32\drivers\etc\ 文件夹中。
   ii. 使用文本编辑器打开hosts文件。

iii. 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：

```
# localhost name resolution is handled within DNS itself.
#       127.0.0.1       localhost
#       ::1             localhost

180.97.161.173  www.aliyundemo.com
```

> **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。

iv. 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。

4.1.7. 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。

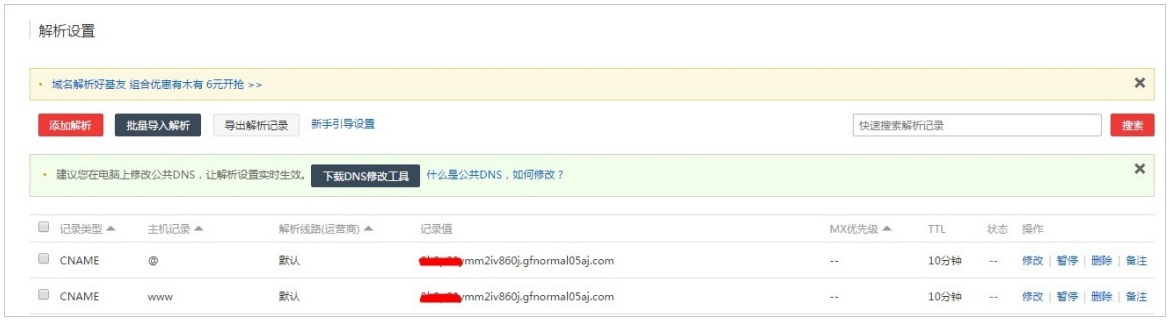
以图中的域名aliyundemo.com为例，当前的域名解析采用A记录的方式，默认线路（除联通以外的线路，包含电信、移动、教育网、铁通、海外等线路）的@和www记录（即用户直接访问域名“aliyundemo.com”或者“www.aliyundemo.com”）都是解析到源站IP地址为11.11.11.11的服务器，而联通线路则是解析到源站IP地址为22.22.22.22的服务器。

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。

4.2. 防护非网站业务

4.2.1. 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。

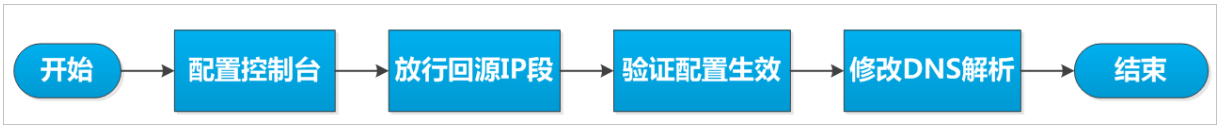
> **说明** 与网站业务不同，非网站业务配置后只进行四层转发。DDoS高防不会解析七层报文的内容，也不提供基于七层报文的防护（如CC攻击、Web攻击等），只支持四层防护（如SYN Flood、UDP Flood等）。

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。

4.2.2. 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。

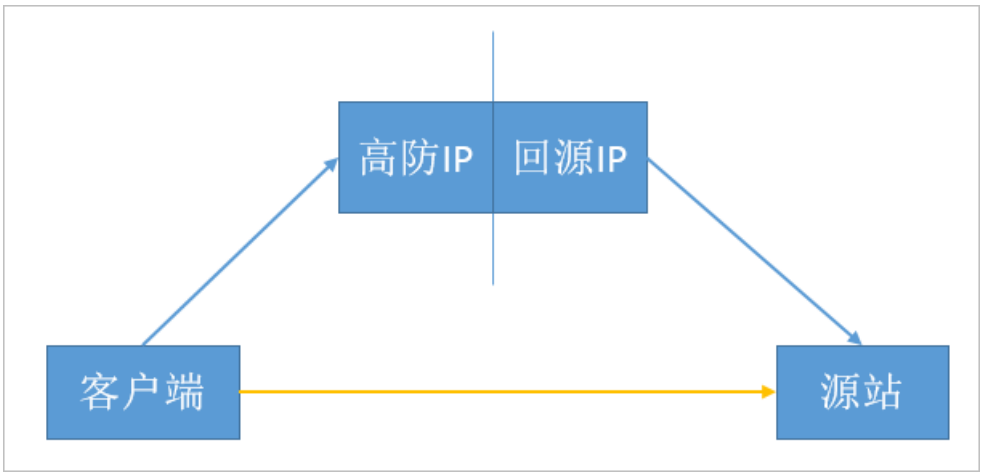
4. 单击**确定**。

4.2.3. 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。

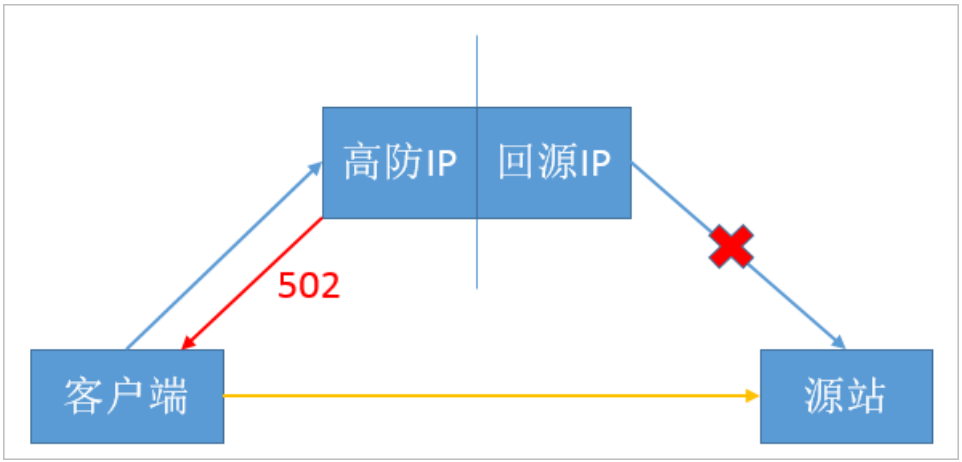
DDoS高防作为一个反向代理，其中包含了一个Full NAT的架构。



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。

4.2.4. 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
  i. 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. 使用文本编辑器打开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：

     ```
     # localhost name resolution is handled within DNS itself.
     #       127.0.0.1       localhost
     #       ::1             localhost

     180.[redacted].173  www.aliyundemo.com
     ```

     d. 修改hosts文件后保存。

  ii. 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。）

  iii. 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。

4.2.5. （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。

5.用户指南

5.1. 业务接入配置

5.1.1. 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。

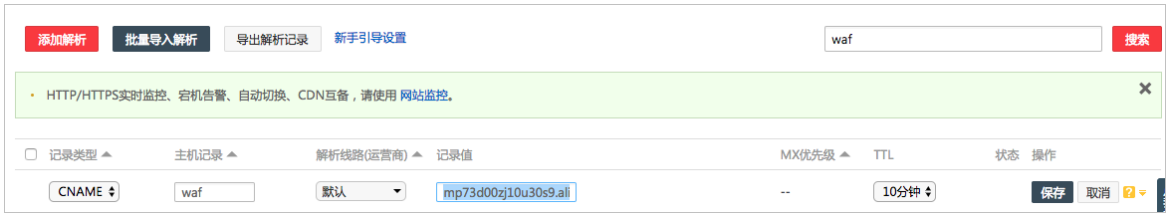
CNAME接入有什么好处？

- 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

5.1.2. 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

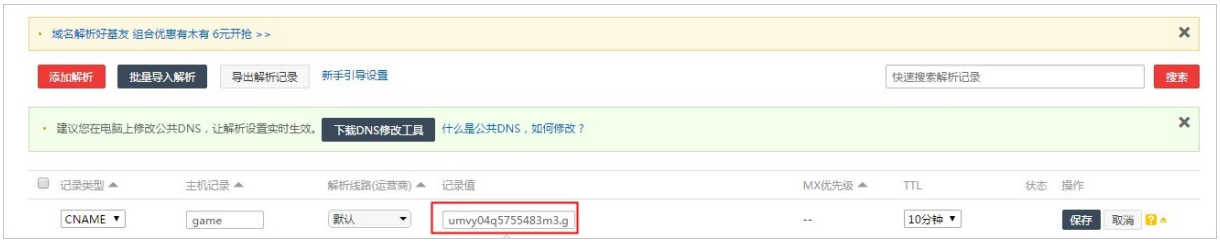
此处的配置方式不变，按照非网站接入的配置方法配置转发规则即可。

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。

5.1.3. 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。

5.1.4. 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，请参见流量调度方式管理。

5.1.5. 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。

5.1.6. 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

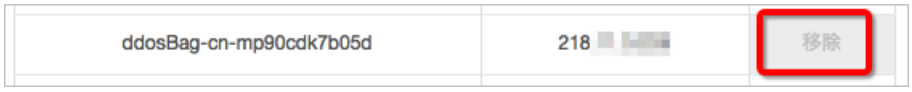
a. 选择已配置的转发线路，单击**编辑线路**，可修改该转发线路所对应的高防IP线路。

- 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**。

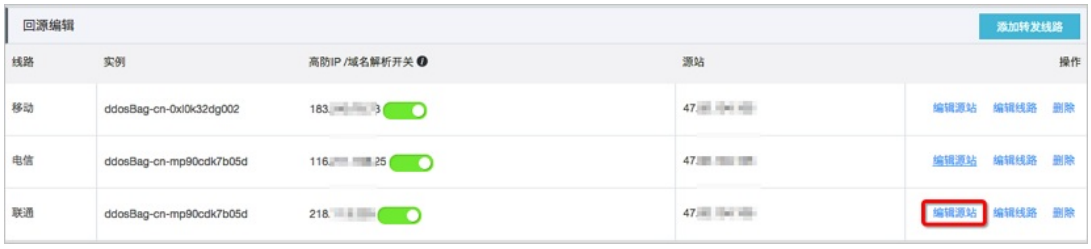
> **说明** 如果某个高防IP实例对应的**移除**显示为灰色，表示该转发线路已经启用该高防IP实例且域名解析开关已开启。



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。

5.1.7. 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。

5.2. 网络七层防护设置

5.2.1. CC攻击防护设置

DDoS高防IP服务针对CC攻击提供四种防护模式供您选择。

CC攻击防护模式说明如下：

- 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. 在左侧导航栏，选择**接入 > 网站**。
3. 单击**防护设置**。
4. 定位到**CC安全防护**区域，选择CC安全防护模式。

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CC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**区域，启用自定义规则防护，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CC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。

5.2.2. 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。

5.2.3. 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。

5.2.4. 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。

5.2.5. 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。

5.3. 网络四层防护设置

5.3.1. 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**。

执行结果

清洗模式调整后在数分钟内即可生效。

5.3.2. 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。

DDoS防护策略配置项	说明
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。

5.3.3. 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。

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。
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。

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。

5.3.4. 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**。

5.4. 实例管理

5.4.1. 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。

5.4.2. 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。

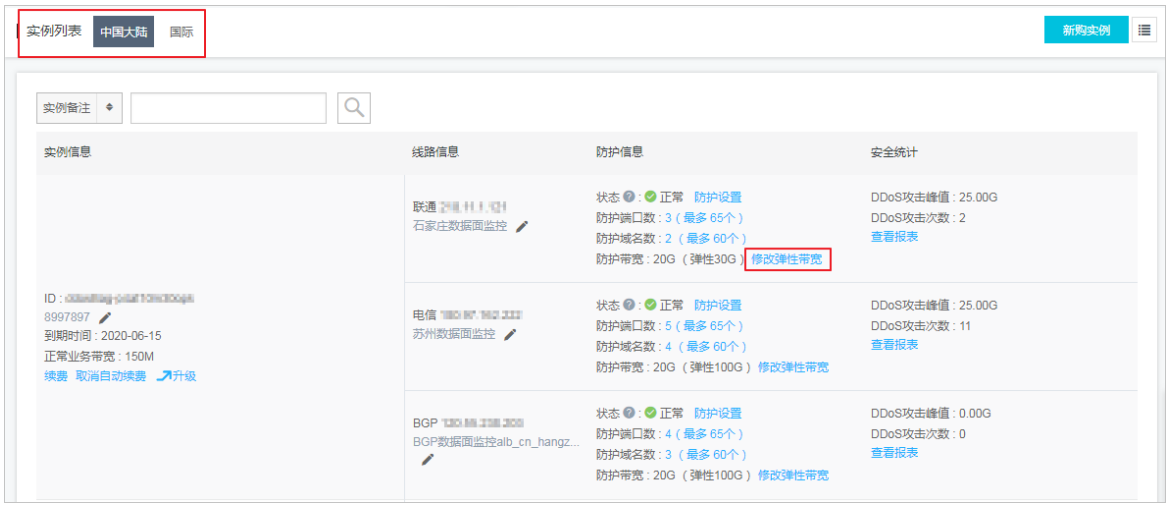
在触发弹性防护（攻击峰值超过保底防护带宽）时，弹性防护根据当天实际发生的攻击峰值生成后付费账单。当天未触发弹性防护时，不产生费用。您可以根据实际业务情况实时调整弹性防护带宽。

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。

5.4.3. 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IP直接攻击源站。您可以在云盾DDoS高防管理控制台更换后端ECS的IP，每个账号最多可更换10次。

前提条件

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。

操作步骤

1. 登录云盾DDoS高防管理控制台。
2. 前往**接入 > 网站**页面，单击**更换ECS IP**。
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。
   i. 在实例列表中找到目标ECS实例，单击其实例ID。
   ii. 在实例详情页，单击**停止**。

iii. 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进行确认。

iv. 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。

5.4.4. 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。

5.5. 统计报表

5.5.1. 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。

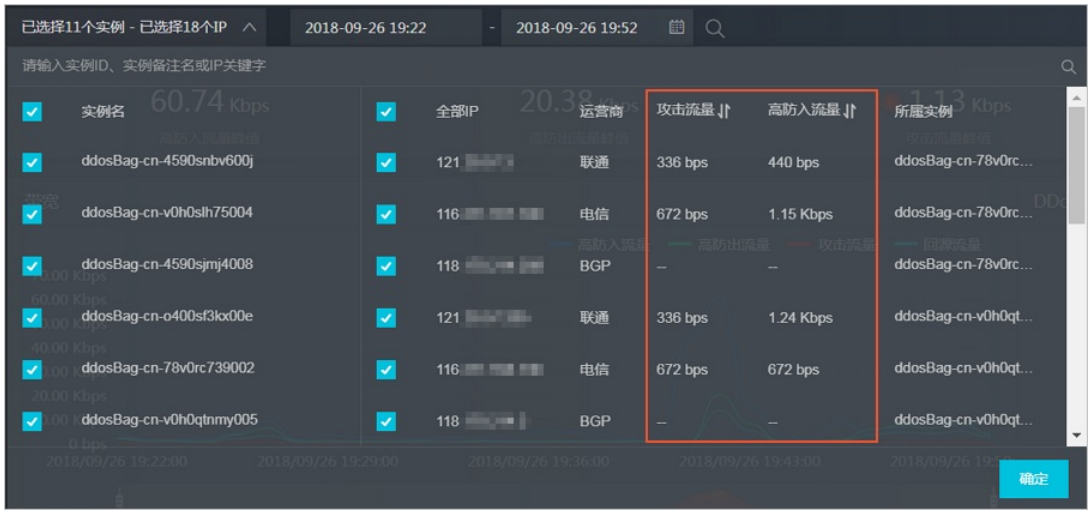
注意 2018年9月27日，DDoS高防IP新安全概览报表功能开启全面公测。公测期间，用户默认最长可查看近一年的攻防数据。

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**。

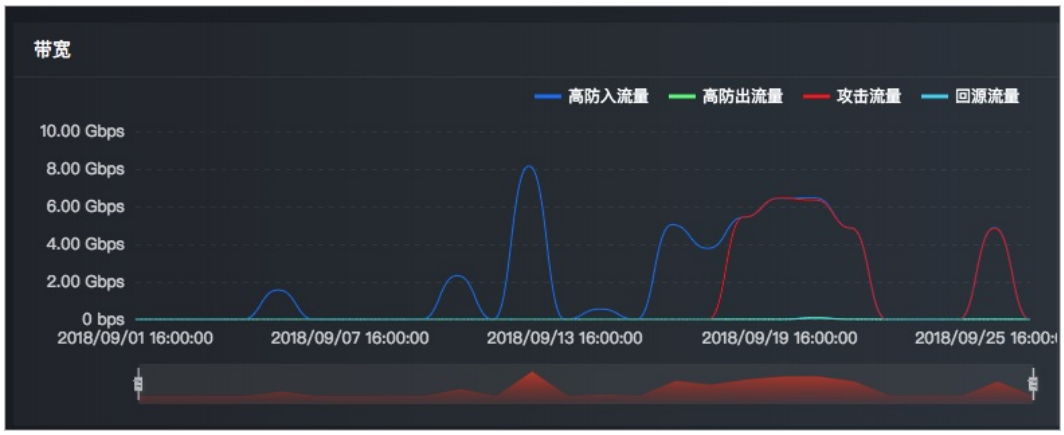
c. 在安全概览报表中，您可以看到以下信息：

- **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。

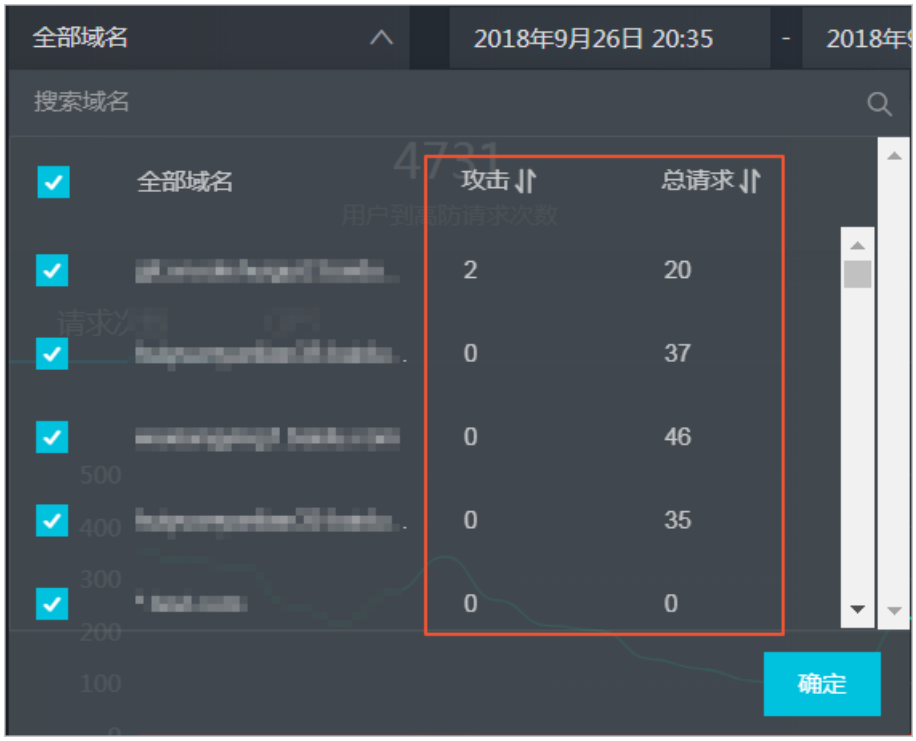
  > **说明** 您可以选择指定端口的连接数据进行展示。

- 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**。

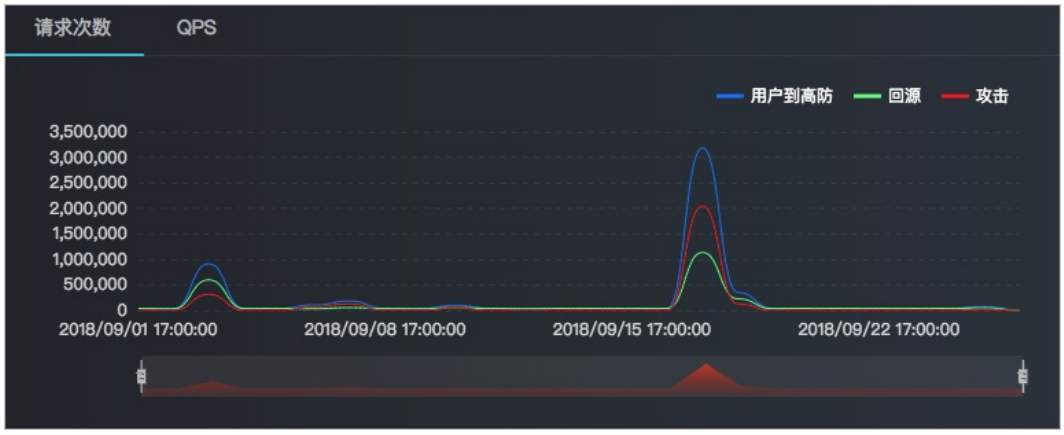
c. 在安全概览报表中，您可以看到以下信息：

- 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。



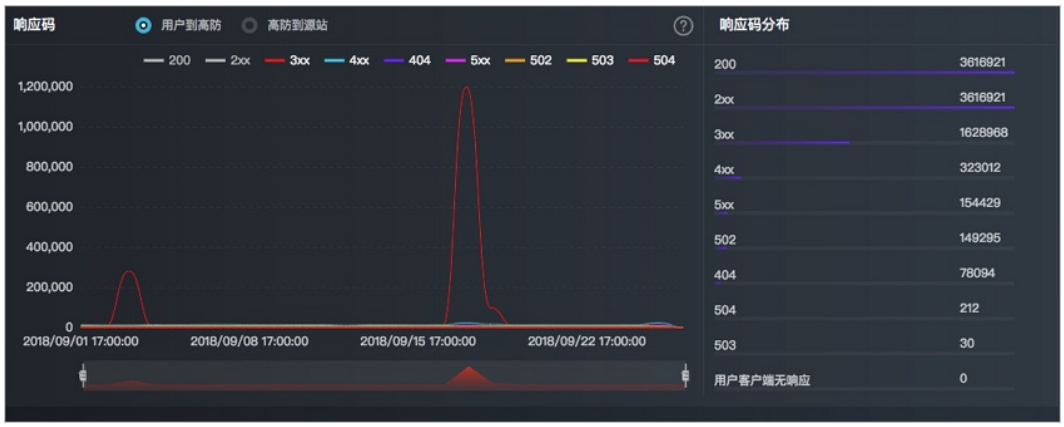
- **CC事件**：查询时间范围内所有CC攻击事件信息。

  > 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。

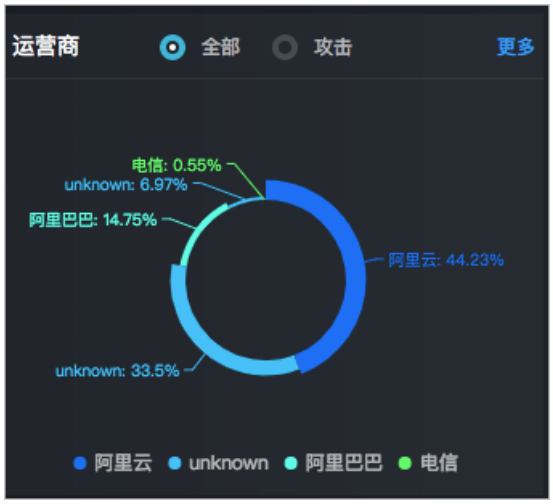
- 全部请求和攻击**请求分布**：查询时间范围内全部请求和攻击请求的分布情况。快速确定网站CC攻击请求的来源分布，可有效辅助您进行下一步的安全防护决策。例如，针对性地封禁海外流量、封禁指定区域IDC的流量等。

  > **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。

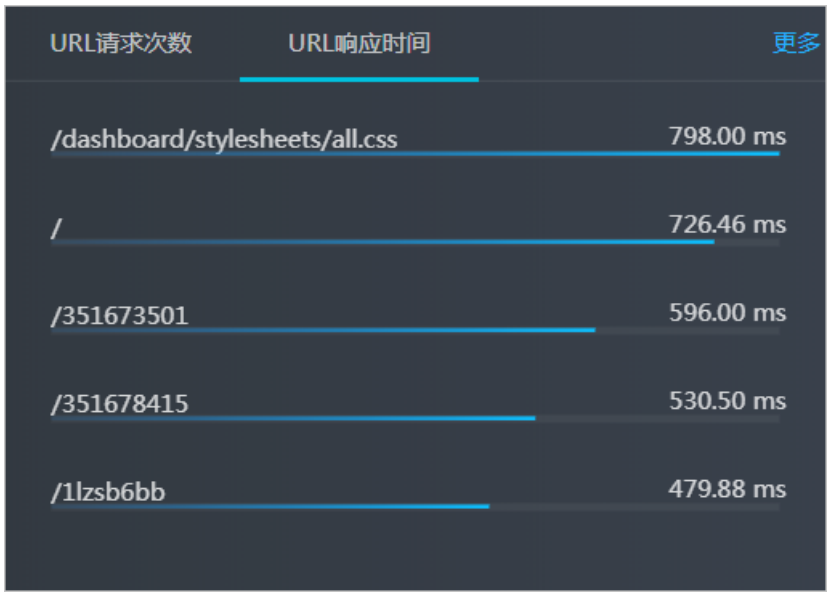


- **运营商**分布：查询时间范围内全部请求或攻击请求的运营商分布情况。



- **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。

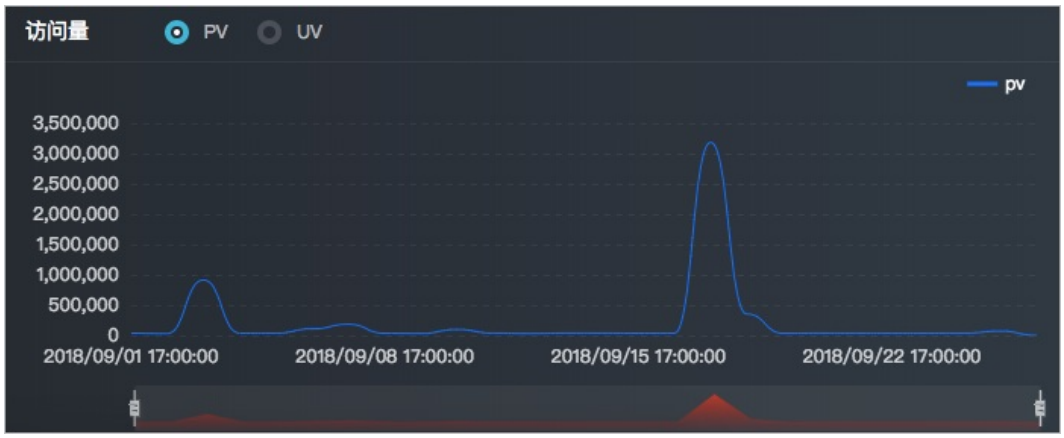


- **浏览器**分布排名：查询时间范围内请求来源的浏览器分布排名。单击**更多**，可查看完整的浏览器排名情况。

- **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。



5.5.2. 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。

5.5.3. 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。

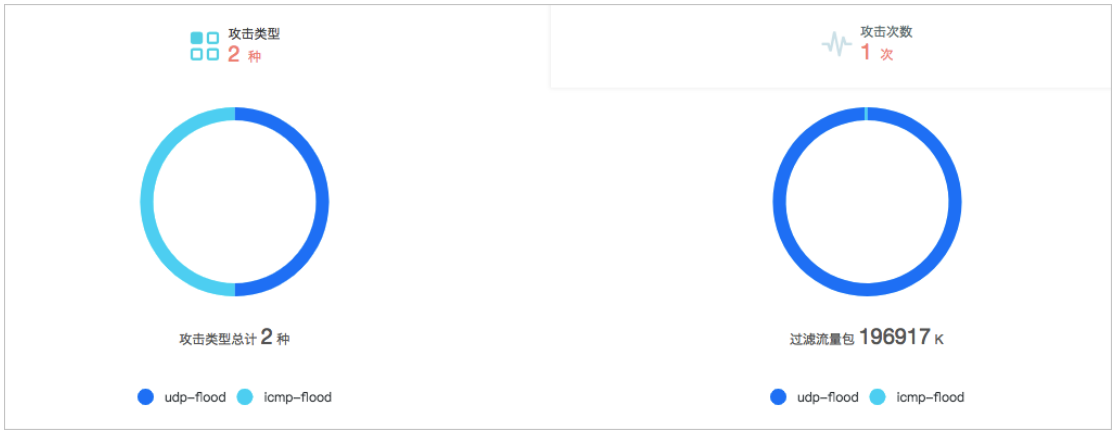
   - 您可以通过单击**攻击类型**和**攻击次数**页签查看攻击详情。

- 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。

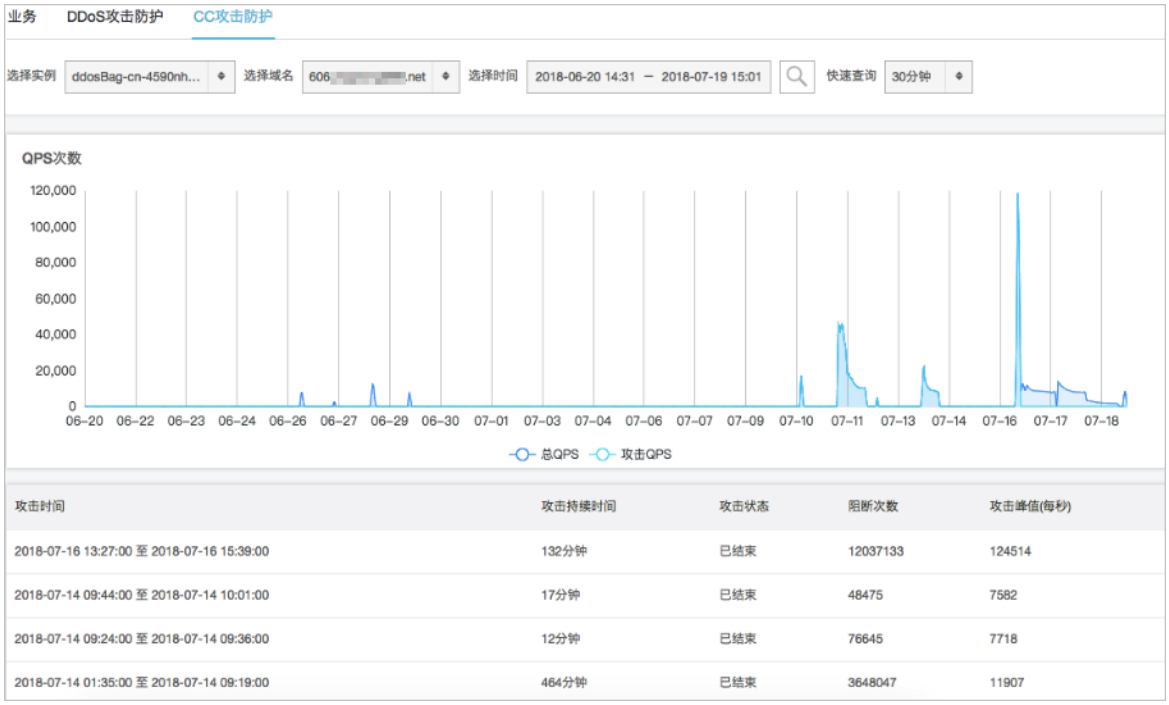
- 攻击类型：查看该时间段内检测到的攻击类型，以及各攻击类型的流量清洗报文数量，帮助辨别当前流量型攻击的攻击类型分布情况。

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。

5.5.4. 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。

执行结果

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。

5.6. 日志查询

5.6.1. 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：

> **注意** 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100 GB/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96 GB/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。

1. 登录云盾DDoS防护管理控制台。
2. 在左侧导航栏，选择**日志 > 全量日志**。
3. 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。

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。

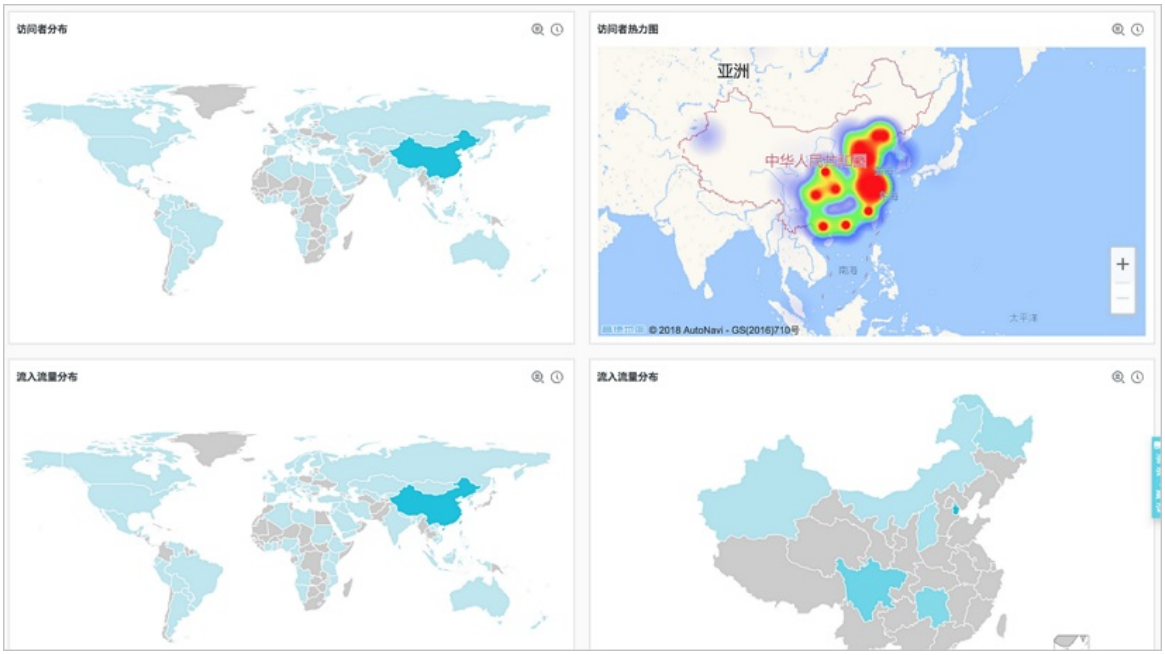
  您可以通过以下语句查看网站访问日志：

  ```
  __topic__: DDoS_access_log
  ```

- 追踪CC攻击者来源

- 您可以通过以下语句分析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
```



- 您可以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。

  您可以通过以下语句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_length)/1024.0/1024.0, 3) as mb_in group by provider having ip_to_provider(if(real_client_ip='-', remote_addr, real_client_ip)) <> '' order by mb_in desc limit 10
```

5.6.2. 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	-

操作日志内容	支持情况	备注
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	-

5.7. 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。

6.最佳实践

6.1. 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。

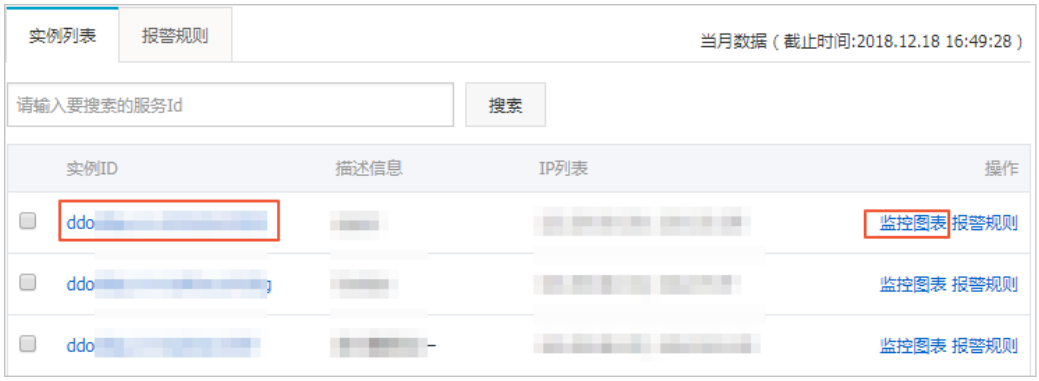
背景信息

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。

6.2. 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

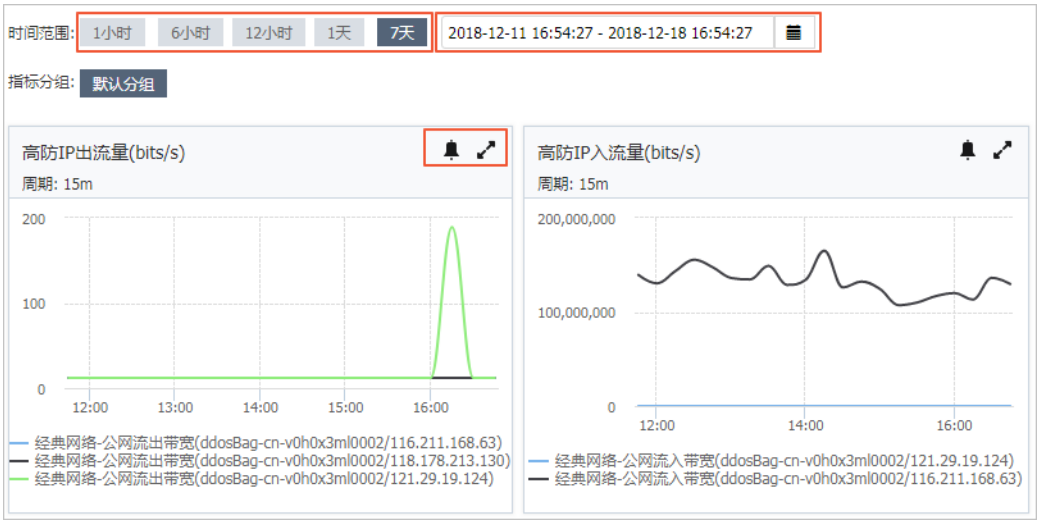
说明 高防IP回源带宽是指通过高防清洗后回源到源站服务器的干净业务流量带宽。

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。

6.3. 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。

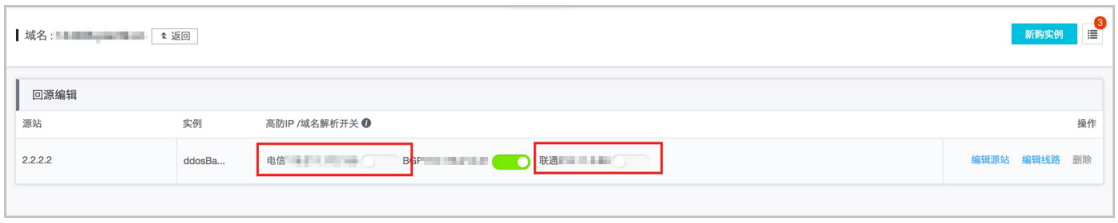
背景信息

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。
   i. 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。



   ii. 单击操作列下的**编辑线路**。

iii. 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。

iv. 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。

i. 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。

ii. 选择启用高防 IP 实例的电信线路，单击**确定**。

iii. 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。

6.4. 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。

7.常见问题

7.1. 配置DDoS高防后业务访问报502错误

概述

本文主要介绍配置DDoS高防后业务访问报502错误的排查思路。

详细信息

- 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。
- 核实负载均衡健康检查是否有异常。
- 如果直接解析到SLB访问正常，需要核实DDoS高防配置是否异常。

> **说明** 测试人员应满足以下要求：
> - 充分了解DDoS高防以及SLB的具体配置。
> - 熟悉SLB的健康检查配置。
> - 熟悉DDoS高防回源的基本原理。

适用于

- 云安全防御

7.2. BGP高防是什么？有什么优势？

BGP协议是什么？

BGP协议指边界网关协议（Border Gateway Protocol），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。

BGP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带宽是中国内地地域目前最昂贵的、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10 M独享带宽的速度，通过BGP只需要5 M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吗？

需要。BGP线路资源宝贵，其基础防护带宽上限只有20 Gbps，而电信、联通线路的基础防护带宽最大可达300 Gbps（弹性防护带宽最大可达600 Gbps）。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？

如果购买单线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，请参见阿里云黑洞策略。

如果购买三线高防（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。更多信息，请参见CNAME自动调度。

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，请参见高防IP服务接入快速入门。

7.3. 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。

7.4. 中国香港线路备用IP使用说明

中国香港线路的备用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。

7.5. 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线路和中国香港线路。

- 电信线路、联通线路、BGP线路需要完成工信部ICP备案，取得备案号才可使用高防IP服务。
- 中国香港线路面向源站在中国香港及东南亚地区的用户，不需要备案。

> **说明** 如果源站服务器部署在大陆地区，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，请参见ICP备案。

> **说明** 源站在中国大陆地区的网站不建议使用中国香港线路的高防IP进行防护，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。

8.视频专区