ALIBABA CLOUD

阿里云

# DDoS防护

# DDoS高防（新BGP&国际）用户指南

文档版本：20220126

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<br>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<br>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<br>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<br>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`<br>*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.购买DDoS高防实例

本文介绍了购买DDoS高防（新BGP）专业版实例、DDoS高防（国际）保险版或无忧版实例、DDoS高防（国际）加速线路、DDoS高防（国际）安全加速线路的操作方法。

## 选择实例类型

您可以根据业务服务器的部署地域和业务主要用户的来源地域，选择要购买哪种类型的DDoS高防实例，具体说明如下：

- 如果您的业务服务器部署在**中国内地**，您需要购买DDoS高防（新BGP）专业版实例。

  > 注意
  > - DDoS高防（新BGP）实例不支持接入未经ICP备案的域名。如果您需要使用DDoS高防（新BGP）防护网站业务，请确认网站域名已经完成ICP备案。更多信息，请参见ICP备案流程概述。
  > - DDoS高防（新BGP）实例默认提供IPv4高防IP。如果您需要IPv6高防IP，请提交工单或者联系销售人员，申请IPv6接入测试。
  >
  >   IPv6高防IP支持转发来自IPv6客户端的请求，对接入业务有以下限制：域名接入只支持IPv4源站，端口接入可以支持IPv4或IPv6源站。

- 如果您的业务服务器部署在**中国内地以外**地域，且业务主要用户来自**中国内地以外**地域，您需要购买DDoS高防（国际）保险版或无忧版实例。
- 如果您的业务服务器部署在**中国内地以外**地域，且业务主要用户来自**中国内地**，由于单独使用DDoS高防（国际）保险版或无忧版不能保障中国内地用户的访问质量（存在约300毫秒的平均访问延时），建议您考虑以下方案：
  - 如果只需要保障中国内地地域电信、联通和非移动线路用户的业务访问速度和稳定性，您可以单独购买DDoS高防（国际）安全加速线路。

    > **说明** 该方案无需您购买DoS高防（国际）保险版或无忧版实例，因为DDoS高防（国际）安全加速线路本身包含DDoS攻击防护和业务访问加速服务。更多信息，请参见配置DDoS高防（国际）安全加速。

  - 如果上述方案不能满足您的需求，建议您同时购买DDoS高防（国际）保险版或无忧版实例，和DDoS高防（国际）加速线路（无防护）。

    > **说明** 该方案需要您使用流量调度器功能配置**出海加速**规则，在无DDoS攻击时，中国内地用户访问被防护业务时，使用加速线路IP，实现访问加速；发生DDoS攻击时，中国内地用户访问被防护业务时，切换使用DDoS高防（国际）保险版或无忧版IP，实现DDoS攻击防护。更多信息，请参见概述。

## 实例连接数规格说明

DDoS高防（新BGP）实例和DDoS高防（国际）实例的默认连接数规格如下：

- 新建连接数：不超过10万/实例
- 并发连接数：不超过100万/实例

> **说明** DDoS高防（新BGP）实例的新建和并发连接数规格会平均分配到中国电信、移动和联通三个运营商线路上。

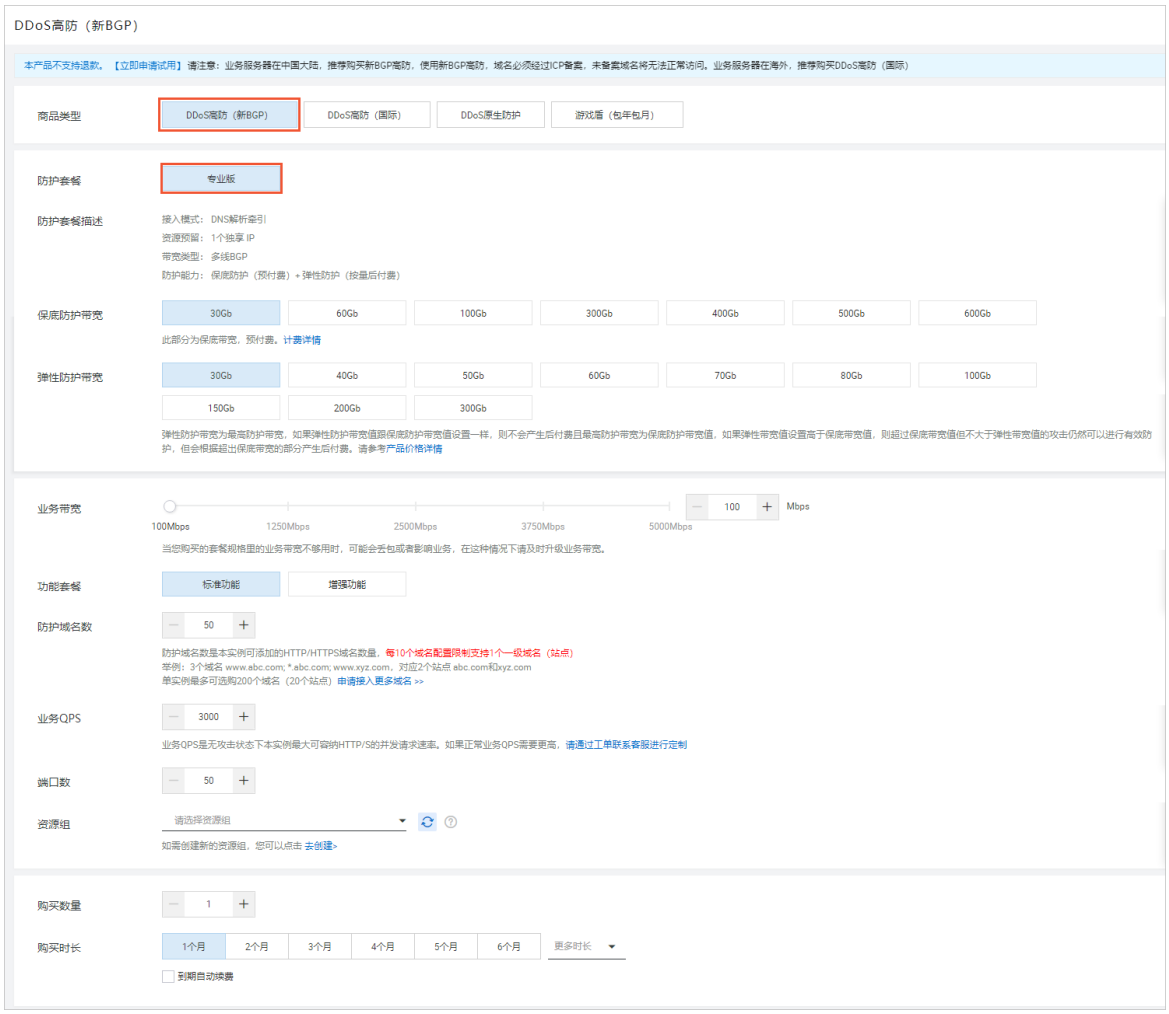
## 购买DDoS高防（新BGP）实例

关于DDoS高防（新BGP）实例的计费方式，请参见DDoS高防（新BGP）计费方式。

> **注意** 本产品一经购买，不支持退款。

参照以下步骤，购买DDoS高防（新BGP）实例：

1. 访问DDoS高防（新BGP）购买页面，并登录您的阿里云账号。
2. 根据您的业务需要，配置DDoS高防（新BGP）实例的规格参数。




| 参数 | 描述 |
| --- | --- |
| **商品类型** | 选择**DDoS高防（新BGP）**。 |
| **防护套餐** | 默认为**专业版**。 |

| 参数 | 描述 |
| --- | --- |
| **保底防护带宽** | 选择实例的保底防护带宽。可选项：30 Gb、60 Gb、100 Gb、300 Gb、400 Gb、500 Gb、600 Gb。<br>保底防护需要预付费后生效。保底防护带宽越大，实例配置费用越高。 |
| **弹性防护带宽** | 选择实例的弹性防护带宽。弹性防护带宽不小于保底防护带宽，且保底防护带宽越大，支持的弹性防护带宽也越大。 可选项：<br>○ 保底防护带宽为30 Gb，弹性防护带宽可设置为：30 Gb、40 Gb、50 Gb、60 Gb、70 Gb、80 Gb、100 Gb、150 Gb、200 Gb、300 Gb。<br>○ 保底防护带宽为60 Gb，弹性防护带宽可设置为：60 Gb、70 Gb、80 Gb、100 Gb、150 Gb、200 Gb、300 Gb、400 Gb、500 Gb、600 Gb。<br>○ 保底防护带宽为100 Gb，弹性防护带宽可设置为：100 Gb、150 Gb、200 Gb、300 Gb、400 Gb、500 Gb、600 Gb。<br>○ 保底防护带宽为300 Gb，弹性防护带宽可设置为：300 Gb、400 Gb、500 Gb、600 Gb、全力防护。<br>○ 保底防护带宽为400 Gb，弹性防护带宽可设置为：400 Gb、500 Gb、600 Gb、全力防护。<br>○ 保底防护带宽为500 Gb，弹性防护带宽可设置为：500 Gb、600 Gb、全力防护。<br>○ 保底防护带宽为600 Gb，弹性防护带宽可设置为：600 Gb、全力防护。<br>弹性防护使用按量后付费的方式计费。弹性防护带宽决定实例的最高防护带宽。具体说明如下：<br>○ 如果**弹性防护带宽**和**保底防护带宽**一样，则最高防护带宽为**保底防护带宽**且不会产生后付费。<br>○ 如果**弹性防护带宽**高于**保底防护带宽**，则超过**保底防护带宽**但不大于**弹性防护带宽**的攻击仍然可以进行有效防护，但会根据超出**保底防护带宽**部分的攻击峰值产生后付费账单。<br>购买实例后，您可以根据实际防护需要，在控制台修改实例的弹性防护带宽。相关操作，请参见修改弹性防护带宽。 |
| **资源组** | 选择实例在资源管理服务中所属的资源组，默认为**默认资源组**。<br>关于资源组的更多信息，请参见创建资源组。 |

| 参数 | 描述 |
| --- | --- |
| **业务带宽** | 选择实例支持处理的正常业务的网络带宽。取值范围：100~5000 Mbps。<br>您可以根据所有将要接入DDoS高防实例的业务的日常入方向或出方向总流量的峰值，选择合适的业务带宽规格。您选择的最大业务带宽应大于这些业务的网络入、出方向总流量峰值中较大的值。一般情况下，网络出方向的流量会比较大。<br>**警告** 如果您购买的实例业务带宽不够用，可能会丢包或者影响业务，在这种情况下请及时升级业务带宽。<br>您可以参考云服务器（ECS）管理控制台中的流量统计，或者通过您业务源站服务器上的其他流量监控工具来评估您的实际业务流量大小。此处的流量指的是正常的业务流量。例如，您将业务的外部访问流量均接入DDoS高防进行防护。在业务正常访问（未遭受攻击）时，DDoS高防将这些正常访问流量回源到源站服务器；而当业务遭受攻击时，DDoS高防过滤、拦截异常流量后，仅将正常流量回源到源站服务器。因此，您在云服务器（ECS）管理控制台中查看您源站服务器的入方向及出方向的流量即是正常的业务流量。如果您的业务部署在多台源站服务器，则需要统计所有源站服务器的流量总和。<br>  <br>假设您需要将三个网站业务接入DDoS高防实例进行防护，每个业务出方向的正常业务流量峰值均不超过50 Mbps，业务流量总和不超过150 Mbps。这种情况下，您只需确保所购买的实例的最大业务带宽大于150 Mbps即可。 |
| **功能套餐** | 选择实例的功能套餐类型。可选项：**标准功能**、**增强功能**。<br>关于不同功能套餐的差异说明，请参见DDoS高防（新BGP&国际）功能套餐。 |
| **防护域名数** | 选择支持接入实例防护的域名配置的数量。支持以10个域名配置为单位增加或减少。可选范围：50~200。<br>域名配置中支持使用子域名、泛域名，且子域名、泛域名对应不同域名的数量不超过“**防护域名数**/10”。<br>例如，默认**防护域名数**为50，表示支持接入最多5个不同的域名对应的子域名、泛域名配置，且所有域名配置的总数不超过50个。<br>假设要接入防护的域名包括aliyundoc.com、aliyun.com，则支持使用上述域名的子域名（例如www.aliyundoc.com、abc.aliyun.com）、泛域名（*.aliyundoc.com、*.aliyun.com）作为域名接入配置。<br>如果需要接入的域名配置的总数超过50，或者域名配置对应的域名数量超过5个，建议您根据需要增加防护域名数规格。 |

| 参数 | 描述 |
| --- | --- |
| **业务QPS** | 选择无攻击状态下实例最大可处理的并发请求速率，包含使用HTTP协议和HTTPS协议的请求。可选范围：3000~100000。<br>**警告** 如果您购买的实例业务QPS不够用，可能会丢包或者影响业务，在这种情况下请及时升级业务QPS。 |
| **防护端口数** | 选择实例支持接入的端口转发配置的数量，包含使用TCP和UDP协议添加的端口转发配置。可选范围：50~400。 |
| **购买数量** | 选择要购买的实例的数量。 |
| **购买时长** | 选择要购买的实例的有效期。可选项：1个月、2个月、3个月、4个月、5个月、6个月、1年、2年。<br>如果选中**到期自动续费**，则在实例到期前自动触发续费。自动续费周期遵循以下规则：<br>○ 按月购买时自动续费周期为一个月。<br>○ 按年购买时自动续费周期为一年。<br>关于自动续费的更多信息，请参见开启自动续费。 |

3. 确认当前配置并单击**立即购买**。
4. 确认订单并完成支付。

## 购买DDoS高防（国际）保险版或无忧版实例

关于DDoS高防（国际）保险版或无忧版实例的计费方式，请参见保险版和无忧版计费方式。

**注意** 本产品一经购买，不支持退款。

参照以下步骤，购买DDoS高防（国际）保险版或无忧版实例：

1. 访问DDoS高防（国际）购买页面，并登录您的阿里云账号。
2. 根据您的业务需要，配置DDoS高防（国际）实例的规格参数。


| 参数 | 描述 |
| --- | --- |
| **商品类型** | 选择**DDoS高防（国际）**。 |
| **防护套餐** | 选择**保险防护**（表示保险版实例）或者**无限防护**（表示无忧版实例）。<br>关于保险版和无忧版的差异说明，请参见保险版和无忧版计费方式。<br>**说明**<br>○ 如果您需要购买加速线路，请参见购买DDoS高防（国际）加速线路。<br>○ 如果您需要购买安全加速线路，请参见购买DDoS高防（国际）安全加速线路。 |

| 参数 | 描述 |
| --- | --- |
| **业务带宽** | 选择实例支持处理的正常业务的网络带宽。可选项：100 Mbps、150 Mbps、200 Mbps、250 Mbps、300 Mbps。<br>您可以根据所有将要接入DDoS高防实例的业务的日常入方向或出方向总流量的峰值，选择合适的业务带宽规格。您选择的最大业务带宽应大于这些业务的网络入、出方向总流量峰值中较大的值。一般情况下，网络出方向的流量会比较大。<br>**警告** 如果您购买的实例业务带宽不够用，可能会丢包或者影响业务，在这种情况下请及时升级业务带宽。<br>您可以参考云服务器（ECS）管理控制台中的流量统计，或者通过您业务源站服务器上的其他流量监控工具来评估您的实际业务流量大小。此处的流量指的是正常的业务流量。例如，您将业务的外部访问流量均接入DDoS高防进行防护。在业务正常访问（未遭受攻击）时，DDoS高防将这些正常访问流量回源到源站服务器；而当业务遭受攻击时，DDoS高防过滤、拦截异常流量后，仅将正常流量回源到源站服务器。因此，您在云服务器（ECS）管理控制台中查看您源站服务器的入方向及出方向的流量即是正常的业务流量。如果您的业务部署在多台源站服务器，则需要统计所有源站服务器的流量总和。<br>  <br>假设您需要将三个网站业务接入DDoS高防实例进行防护，每个业务出方向的正常业务流量峰值均不超过50 Mbps，业务流量总和不超过150 Mbps。这种情况下，您只需确保所购买的实例的最大业务带宽大于150 Mbps即可。 |
| **功能套餐** | 选择实例的功能套餐类型。可选项：**标准功能**、**增强功能**。<br>关于不同功能套餐的差异说明，请参见DDoS高防（新BGP&国际）功能套餐。 |
| **防护域名数** | 选择支持接入实例防护的域名配置的数量。支持以10个域名配置为单位增加或减少。可选范围：10~200。<br>域名配置中支持使用子域名、泛域名，且子域名、泛域名对应不同域名的数量不超过“**防护域名数**/10”。<br>例如，默认**防护域名数**为10，表示支持接入最多1个不同的域名对应的子域名、泛域名配置，且所有域名配置的总数不超过10个。<br>假设要接入防护的域名为aliyundoc.com，则支持使用该域名的子域名（例如www.aliyundoc.com、abc.aliyundoc.com）、泛域名（*.aliyundoc.com）作为域名接入配置。<br>如果需要接入的域名配置的总数超过10，或者域名配置对应的域名数量超过1个，建议您根据需要增加**防护域名数**规格。 |

| 参数 | 描述 |
| --- | --- |
| **业务QPS** | 选择无攻击状态下实例最大可处理的并发请求速率，包含使用HTTP协议和HTTPS协议的请求。可选范围：<br>○ 保险版：500~100000<br>○ 无忧版：1000~100000<br>**警告** 如果您购买的实例业务QPS不够用，可能会丢包或者影响业务，在这种情况下请及时升级业务QPS。 |
| **防护端口数** | 选择实例支持接入的端口转发配置的数量，包含使用TCP和UDP协议添加的端口转发配置。可选范围：5~400。 |
| **购买数量** | 选择要购买的实例的数量。 |
| **购买时长** | 选择要购买的实例的有效期。可选项：3个月、6个月、1年、2年。<br>如果选中**到期自动续费**，则在实例到期前自动触发续费。自动续费周期遵循以下规则：<br>○ 按月购买时自动续费周期为一个月。<br>○ 按年购买时自动续费周期为一年。<br>关于自动续费的更多信息，请参见开启自动续费。 |

3. 确认当前配置并单击**立即购买**。
4. 确认订单并完成支付。

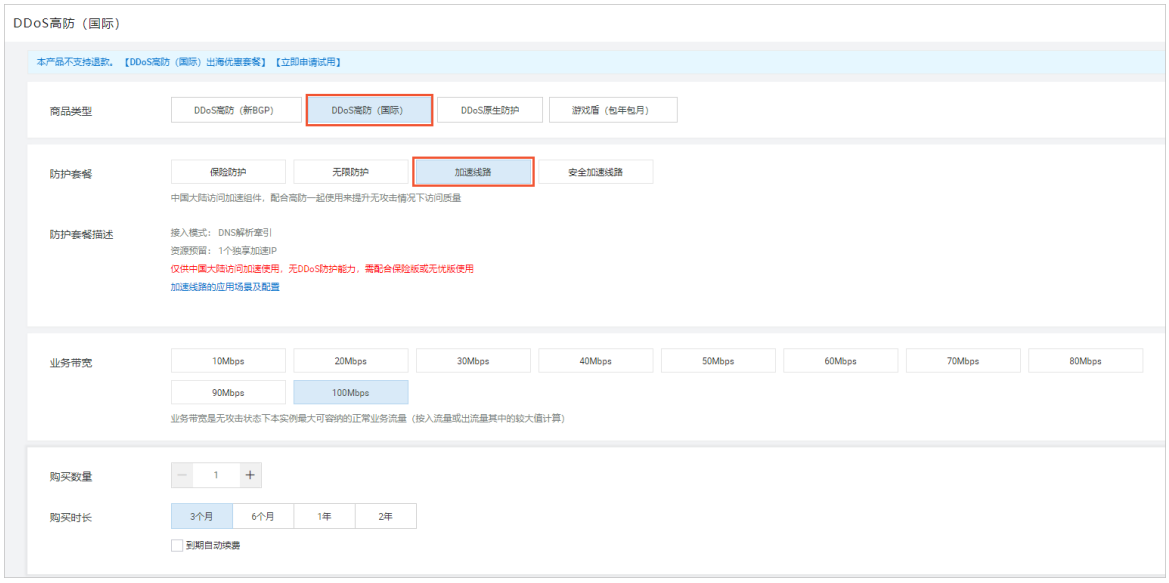
## 购买DDoS高防（国际）加速线路

关于DDoS高防（国际）加速线路的计费方式，请参见加速线路计费方式。

**注意** 本产品一经购买，不支持退款。

参照以下步骤，购买DDoS高防（国际）加速线路：

1. 访问DDoS高防（国际）购买页面，并登录您的阿里云账号。
2. 根据您的业务需要，配置DDoS高防（国际）加速线路的规格参数。




| 参数 | 描述 |
| --- | --- |
| **商品类型** | 选择**DDoS高防（国际）**。 |
| **防护套餐** | 选择**加速线路**。 |
| **业务带宽** | 选择实例支持处理的正常业务的网络带宽。可选项：10 Mbps、20 Mbps、30 Mbps、40 Mbps、50 Mbps、60 Mbps、70 Mbps、80 Mbps、90 Mbps、100 Mbps。<br>您可以根据所有将要接入DDoS高防实例的业务的日常入方向或出方向总流量的峰值，选择合适的业务带宽规格。您选择的最大业务带宽应大于这些业务的网络入、出方向总流量峰值中较大的值。一般情况下，网络出方向的流量会比较大。<br>**警告** 如果您购买的实例业务带宽不够用，可能会丢包或者影响业务，在这种情况下请及时升级业务带宽。<br>您可以参考云服务器（ECS）管理控制台中的流量统计，或者通过您业务源站服务器上的其他流量监控工具来评估您的实际业务流量大小。此处的流量指的是正常的业务流量。例如，您将业务的外部访问流量均接入DDoS高防进行防护。在业务正常访问（未遭受攻击）时，DDoS高防将这些正常访问流量回源到源站服务器；而当业务遭受攻击时，DDoS高防过滤、拦截异常流量后，仅将正常流量回源到源站服务器。因此，您在云服务器（ECS）管理控制台中查看您源站服务器的入方向及出方向的流量即是正常的业务流量。如果您的业务部署在多台源站服务器，则需要统计所有源站服务器的流量总和。<br>  <br><br>假设您需要将三个网站业务接入DDoS高防实例进行防护，每个业务出方向的正常业务流量峰值均不超过50 Mbps，业务流量总和不超过150 Mbps。这种情况下，您只需确保所购买的实例的最大业务带宽大于150 Mbps即可。 |

| 参数 | 描述 |
| --- | --- |
| **购买数量** | 选择要购买的实例的数量。 |
| **购买时长** | 选择要购买的实例的有效期。可选项：3个月、6个月、1年、2年。<br>如果选中**到期自动续费**，则在实例到期前自动触发续费。自动续费周期遵循以下规则：<br>○ 按月购买时自动续费周期为一个月。<br>○ 按年购买时自动续费周期为一年。<br>关于自动续费的更多信息，请参见开启自动续费。 |

3. 确认当前配置并单击**立即购买**。
4. 确认订单并完成支付。

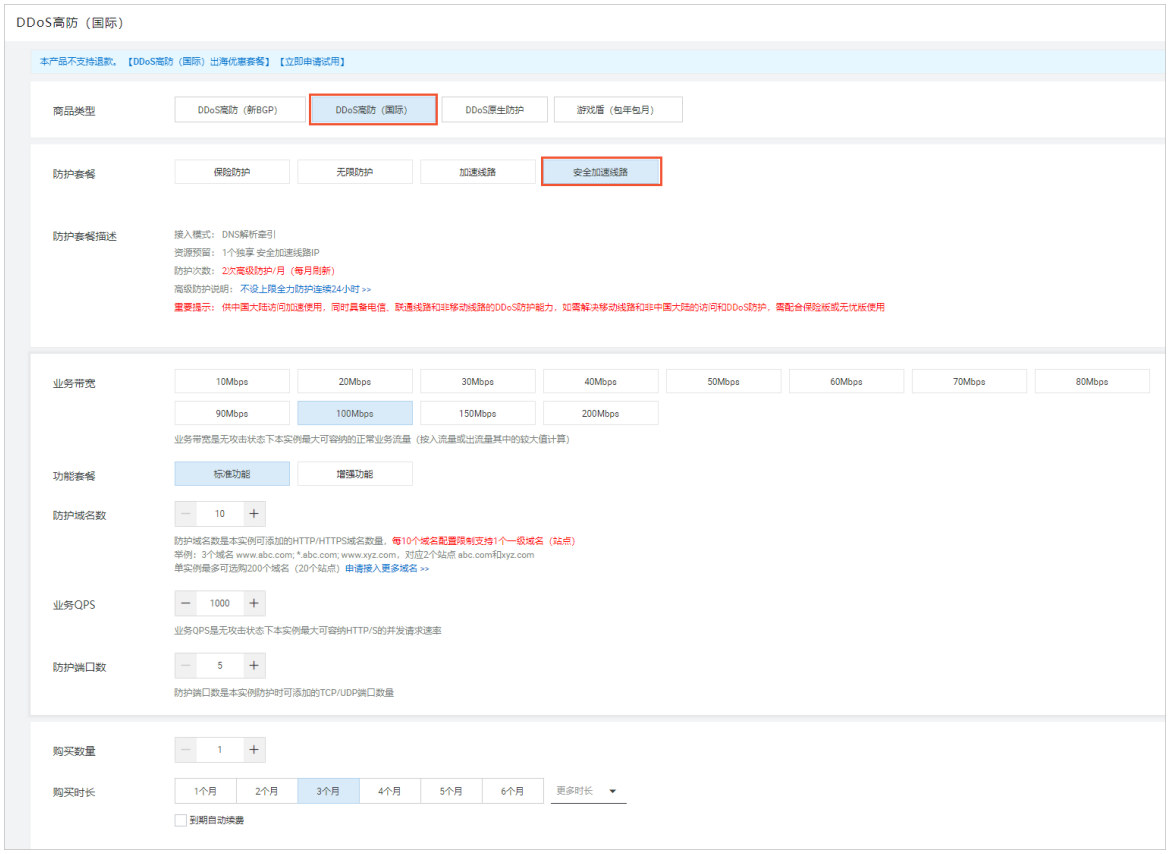
## 购买DDoS高防（国际）安全加速线路

关于DDoS高防（国际）安全加速线路的计费方式，请参见安全加速线路计费方式。

> **注意** 本产品一经购买，不支持退款。

参照以下步骤，购买DDoS高防（国际）安全加速线路：

1. 访问DDoS高防（国际）购买页面，并登录您的阿里云账号。
2. 根据您的业务需要，配置DDoS高防（国际）安全加速线路的规格参数。



| 参数 | 描述 |
| --- | --- |
| **商品类型** | 选择**DDoS高防（国际）**。 |
| **防护套餐** | 选择**安全加速线路**。 |
| **业务带宽** | 选择实例支持处理的正常业务的网络带宽。可选项：10 Mbps、20 Mbps、30 Mbps、40 Mbps、50 Mbps、60 Mbps、70 Mbps、80 Mbps、90 Mbps、100 Mbps、150 Mbps、200 Mbps。<br>您可以根据所有将要接入DDoS高防实例的业务的日常入方向或出方向总流量的峰值，选择合适的业务带宽规格。您选择的最大业务带宽应大于这些业务的网络入、出方向总流量峰值中较大的值。一般情况下，网络出方向的流量会比较大。<br>**警告** 如果您购买的实例业务带宽不够用，可能会丢包或者影响业务，在这种情况下请及时升级业务带宽。<br>您可以参考云服务器（ECS）管理控制台中的流量统计，或者通过您业务源站服务器上的其他流量监控工具来评估您的实际业务流量大小。此处的流量指的是正常的业务流量。例如，您将业务的外部访问流量均接入DDoS高防进行防护。在业务正常访问（未遭受攻击）时，DDoS高防将这些正常访问流量回源到源站服务器；而当业务遭受攻击时，DDoS高防过滤、拦截异常流量后，仅将正常流量回源到源站服务器。因此，您在云服务器（ECS）管理控制台中查看您源站服务器的入方向及出方向的流量即是正常的业务流量。如果您的业务部署在多台源站服务器，则需要统计所有源站服务器的流量总和。<br>  <br>假设您需要将三个网站业务接入DDoS高防实例进行防护，每个业务出方向的正常业务流量峰值均不超过50 Mbps，业务流量总和不超过150 Mbps。这种情况下，您只需确保所购买的实例的最大业务带宽大于150 Mbps即可。 |
| **功能套餐** | 选择实例的功能套餐类型。可选项：**标准功能**、**增强功能**。<br>关于不同功能套餐的差异说明，请参见DDoS高防（新BGP&国际）功能套餐。 |
| **防护域名数** | 选择支持接入实例防护的域名配置的数量。支持以10个域名配置为单位增加或减少。可选范围：10~200。<br>域名配置中支持使用子域名、泛域名，且子域名、泛域名对应不同域名的数量不超过“**防护域名数**/10”。<br>例如，默认**防护域名数**为10，表示支持接入最多1个不同的域名对应的子域名、泛域名配置，且所有域名配置的总数不超过10个。<br>假设要接入防护的域名为aliyundoc.com，则支持使用该域名的子域名（例如www.aliyundoc.com、abc.aliyundoc.com）、泛域名（*.aliyundoc.com）作为域名接入配置。<br>如果需要接入的域名配置的总数超过10，或者域名配置对应的域名数量超过1个，建议您根据需要增加**防护域名数**规格。 |

| 参数 | 描述 |
| --- | --- |
| **业务QPS** | 选择无攻击状态下实例最大可处理的并发请求速率，包含使用HTTP协议和HTTPS协议的请求。可选范围：500~100000。<br>**警告** 如果您购买的实例业务QPS不够用，可能会丢包或者影响业务，在这种情况下请及时升级业务QPS。 |
| **防护端口数** | 选择实例支持接入的端口转发配置的数量，包含使用TCP和UDP协议添加的端口转发配置。可选范围：5~400。 |
| **购买数量** | 选择要购买的实例的数量。 |
| **购买时长** | 选择要购买的实例的有效期。可选项：1个月、2个月、3个月、4个月、5个月、6个月、1年、2年。<br>如果选中**到期自动续费**，则在实例到期前自动触发续费。自动续费周期遵循以下规则：<br>○ 按月购买时自动续费周期为一个月。<br>○ 按年购买时自动续费周期为一年。<br>关于自动续费的更多信息，请参见开启自动续费。 |

3. 确认当前配置并单击**立即购买**。
4. 确认订单并完成支付。

## 相关文档

- 调用API创建DDoS高防实例

# 2.快速入门

## 2.1. 防护网站业务

### 2.1.1. 概览

本文将指导您在开通DDoS高防后，快速部署和使用DDoS高防，为网站业务配置DDoS防护。

使用DDoS高防防护网站业务时，您可以按照以下步骤进行操作。

| 任务 | 描述 |
| --- | --- |
| 步骤1：添加网站业务转发规则 | 在DDoS高防控制台通过域名接入添加要防护的网站业务，关联DDoS高防实例并设置业务流量转发策略。 |
| 步骤2：接入网站业务流量 | 修改已接入DDoS高防的域名的解析记录，将网站业务流量牵引到DDoS高防实例。完成切换后，网站的访问流量都会先经过DDoS高防清洗，再转发到源站服务器，实现由DDoS高防实例帮助网站防御DDoS攻击流量。 |
| 步骤3：设置网站业务防护策略 | 网站业务接入DDoS高防后，默认启用AI智能防护，无需您进行额外操作。在遇到异常情况或有特殊需求时，您可以手动调整网站业务的DDoS防护策略，具体包括AI智能防护、针对域名的黑白名单、针对域名的区域封禁、精确访问控制、频率控制。 |
| 步骤4：查看网站业务防护数据 | 网站业务接入DDoS高防后，您可以在DDoS高防控制台使用安全报表和日志功能查看业务防护数据。<br>**说明** 目前仅DDoS高防（新BGP）服务支持安全报表和操作日志功能。 |

### 2.1.2. 步骤1：添加网站业务转发规则

使用DDoS高防防护网站业务时，您必须首先在DDoS高防中添加要防护的域名，设置业务流量的转发策略。

#### 前提条件

已开通DDoS高防（新BGP/国际）实例。更多信息，请参见购买DDoS高防实例。

#### 背景信息

**注意** DDoS高防控制台在顶部导航栏新增地域切换菜单，方便您切换选择DDoS高防（新BGP）、DDoS高防（国际）服务。地域切换菜单支持**中国内地**和**非中国内地**选项，您可以通过切换地域分别管理和配置DDoS高防（新BGP）和DDoS高防（国际）实例。在使用DDoS高防服务时，请确认您已选择正确的地域。

本文以DDoS高防（新BGP）服务为例描述具体操作。如果您使用DDoS高防（国际）服务，请参见添加网站。

#### 操作步骤

1. 登录DDoS高防控制台。

2. 在顶部导航栏，选择**中国内地**地域。
3. 在左侧导航栏，选择**接入管理 > 域名接入**。
4. 在**域名接入**页面，单击**添加网站**。

> **说明** 您也可以批量导入网站配置，具体请参见批量导入网站配置。

5. 按照页面提示，完成**添加网站**配置向导。
   i. **填写网站信息**。


填写以下网站信息，并单击**添加**。

| 参数 | 适用的实例类型 | 说明 |
| --- | --- | --- |

| 参数 | 适用的实例类型 | 说明 |
| --- | --- | --- |
| **功能套餐** | DDoS高防（新BGP）和DDoS高防（国际） | 选择要关联的DDoS高防实例的功能套餐。可选项：**标准功能**、**增强功能**。<br>您可以将光标放置在**功能套餐**后的图标上，查看标准功能和增强功能套餐的功能差异（如下图所示）。<br>  <br>功能分类 / 功能列表 / 标准功能 / 增强功能<br>防护算法：流量型攻击防护（标准功能：✓，增强功能：✓）<br>防护算法：资源耗尽型攻击防护（四七层CC攻击防护）（标准功能：✓，增强功能：✓）<br>防护算法：AI智能防护（标准功能：✓，增强功能：✓）<br>防护规则：黑白名单（标准功能：✓，增强功能：✓）<br>防护规则：精准访问控制（标准功能：5条，支持部分匹配字段；增强功能：10条）<br>防护规则：区域IP封禁（标准功能：×，增强功能：✓）<br>业务接入：HTTP（80/8080），HTTPS（443/8443）转发（标准功能：✓，增强功能：✓）<br>业务接入：HTTP，HTTPS非标端口转发（标准功能：×，增强功能：10个端口）<br>业务接入：TLS协议加密套件自定义（标准功能：×，增强功能：✓）<br>业务接入：HTTP 2.0、HTTPS跳转、HTTP回源和回源负载策略（标准功能：✓，增强功能：✓）<br>其他：静态页面缓存（标准功能：×，增强功能：✓） |
| **实例** | DDoS高防（新BGP）和DDoS高防（国际） | 选择要关联的DDoS高防实例。一个网站域名最多可以关联8个DDoS高防实例，且只能关联同一种**功能套餐**下的多个实例。<br>此处根据您选择的**功能套餐**类型显示对应的DDoS高防实例。如果无可选实例，表示您当前无可用的该功能套餐的DDoS高防实例。您可以新购实例或升级已有的标准功能套餐实例。具体操作，请参见升级实例。 |
| **网站** | DDoS高防（新BGP）和DDoS高防（国际） | 填写要防护的网站域名。具体要求如下：<br>■ 域名可以由26个英文字母（a~z、A~Z，不区分大小写）、数字（0~9）以及短划线（-）组成。域名的首位必须是字母或数字。<br>■ 支持填写泛域名，例如，`*.aliyundoc.com`。使用泛域名时，DDoS高防自动匹配该泛域名对应的子域名。<br>■ 如果同时存在泛域名和精确域名配置（例如，`*.aliyundoc.com` 和 `www.aliyundoc.com`），DDoS高防优先使用精确域名（即 `www.aliyundoc.com`）所配置的转发规则和防护策略。 |

| 参数 | 适用的实例类型 | 说明 |
| --- | --- | --- |
| **协议类型** | DDoS高防（新BGP）和DDoS高防（国际） | 选择网站支持的协议类型。可选项：<br>■ **HTTP**<br>■ **HTTPS**：如果网站支持HTTPS加密认证，请选中**HTTPS**协议，并在保存网站配置后上传网站域名使用的HTTPS证书。关于上传证书的操作，请参见上传HTTPS证书。<br>■ **Websocket**：选中该协议将自动同时选中**HTTP**协议，不支持单独选中**Websocket**协议。<br>■ **Websockets**：选中该协议将自动同时选中**HTTPS**协议，不支持单独选中**Websockets**协议。<br>选中**HTTPS**协议后，您可以根据需要开启以下高级设置：<br>  <br><br>■ **开启HTTPS的强制跳转**：适用于您的网站同时支持HTTP和HTTPS协议。开启该设置后，所有HTTP请求将被强制转换为HTTPS请求，且默认跳转到443端口。<br>**注意**<br>■ 只有当您同时选中**HTTP**和**HTTPS**协议，并且没有选中**Websocket**协议时，才可以开启该设置。<br>■ HTTP非标准端口（80以外的端口）访问的场景下，如果开启了HTTPS强制跳转，则访问默认跳转到HTTPS 443端口。<br>■ **开启HTTP回源**：适用于您的网站不支持HTTPS回源。开启该设置后，所有HTTPS协议请求将通过HTTP协议回源、所有Websockets协议请求将通过Websocket协议回源，且默认回源端口为80。<br>**注意**<br>■ 如果您的网站不支持HTTPS回源，请务必开启该设置。<br>■ HTTPS非标准端口（443以外的端口）访问的场景下，如果开启了HTTP回源，则访问默认跳转到源站HTTP 80端口。<br>■ **启用HTTP2**：开启该设置，表示源站使用了HTTP 2.0协议。 |

| 参数 | 适用的实例类型 | 说明 |
| --- | --- | --- |
| **启用OCSP** | DDoS高防（新BGP）和DDoS高防（国际） | 选择是否启用OCSP（Online Certificate Status Protocol）功能。<br><br>**注意** 该功能适用于网站HTTPS业务。如果您已选择的**协议类型**包含**HTTPS**，推荐您启用该功能。<br><br>OCSP表示在线证书状态协议，该协议用于向签发证书的CA（Certificate Authority）中心发起查询请求，检查证书是否被吊销。在与服务器进行TLS握手时，客户端必须同时获取证书和对应的OCSP响应。<br><br>OCSP功能默认未开启，表示由客户端浏览器向CA中心发起OCSP查询。该方式会导致客户端在获得OCSP响应前阻塞后续的事件，在网络情况不佳时，将造成较长时间的页面空白，降低HTTPS的性能。<br><br>启用OCSP表示由DDoS高防来执行OCSP查询并缓存查询结果（缓存时间为300秒）。当有客户端向服务器发起TLS握手请求时，DDoS高防将证书的OCSP信息随证书链一起发送给客户端，从而避免了客户端查询会产生的阻塞问题。由于OCSP响应是无法伪造的，因此这一过程不会产生额外的安全问题。 |

| 参数 | 适用的实例类型 | 说明 |
| --- | --- | --- |
| **服务器地址** | DDoS高防（新BGP）和DDoS高防（国际） | 选择源站服务器的地址类型，并填写源站服务器的地址。支持的地址类型包括：<br>■ **源站IP**：表示源站服务器的IP地址。最多支持配置20个源站IP地址，多个IP地址间使用半角逗号（,）分隔。<br>示例：<br>■ 如果源站在阿里云，一般填写源站ECS的公网IP地址；如果ECS前面部署了SLB，则填写SLB的公网IP地址。<br>■ 如果源站在阿里云外的IDC机房或者其他云服务商，您可以使用 `ping 域名` 命令，查询域名解析到的公网IP地址，并填写您获取的公网IP。<br>■ **源站域名**：通常适用于源站和高防之间还部署有其他代理服务（例如，Web应用防火墙）的场景，表示代理服务的跳转地址（例如，Web应用防火墙提供给您的CNAME地址）。最多支持配置10个源站域名，多个域名间通过换行分隔。<br>示例：如果您在部署DDoS高防实例后还需要部署Web应用防火墙（WAF），以提升应用安全防护能力，您可以选择**源站域名**类型，并填写WAF的CNAME地址。更多信息，请参见同时部署WAF和DDoS高防。<br>**注意** 如果您设置的**源站域名**为OSS存储空间（Bucket）的默认外网访问域名，则对应存储空间必须已绑定自定义域名。更多信息，请参见绑定自定义域名。<br>配置多个服务器地址（源站IP、源站域名）后，DDoS高防默认以IP Hash的方式转发网站访问流量至源站，自动实现负载均衡。保存网站配置后，您可以通过回源设置，修改源站负载算法。具体操作，请参见修改回源设置。 |

| 参数 | 适用的实例类型 | 说明 |
| --- | --- | --- |
| **服务器端口** | DDoS高防（新BGP）和DDoS高防（国际） | 根据已选择的**协议类型**，设置源站提供对应服务的端口。<br>**HTTP**协议的**服务器端口**默认为80；**HTTPS**协议的**服务器端口**默认为443。<br>**注意**<br>■ Websocket协议的端口与HTTP协议的端口一致。<br>■ Websockets和HTTP 2.0协议的端口与HTTPS协议的端口一致。<br>您可以单击**自定义**，自定义服务器端口。**HTTP**或**HTTPS**协议下均支持自定义多个端口。多个端口间使用半角逗号（,）分隔。<br>  <br>自定义服务器端口有以下要求：<br>■ 自定义端口必须在可选端口范围内。您可以单击**查看可选范围**，查看HTTP或HTTPS协议支持的可选端口范围。<br>DDoS高防实例的**功能套餐**不同，支持的可选端口范围不同，具体说明如下：<br>■ **标准功能**实例：<br>■ HTTP协议可选端口：80、8080。<br>■ HTTPS协议可选端口：443、8443。<br>■ **增强功能**实例：<br>■ HTTP协议可选端口范围：80~65535。<br>■ HTTPS协议可选端口范围：80~65535。<br>■ 所有接入DDoS高防实例防护的网站业务下自定义的不同端口（包含不同协议下的自定义端口）的总数不能超过10个。<br>示例：假设您有2个网站（A和B）要接入DDoS高防实例防护，网站A提供HTTP服务、网站B提供HTTPS服务。<br>如果您在网站A的接入配置中自定义了HTTP 80、8080端口，那么在网站B的接入配置中，您最多可以自定义8个不同的HTTPS端口。 |

| 参数 | 适用的实例类型 | 说明 |
| --- | --- | --- |
| Cname Reuse | DDoS高防（国际） | 选择是否开启CNAME复用。<br>该功能适用于同一台服务器上有多个网站业务的场景。开启CNAME复用后，您只需将同一个服务器上多个域名的解析指向同一个高防CNAME地址，即可将多个域名接入高防，无需为每个域名分别添加高防网站配置。更多信息，请参见CNAME复用。 |

ii. **完成配置**。


按照页面提示，完成以下后续步骤：

a. 放行DDoS高防回源IP：

如果源站服务器上安装了防火墙等安全软件，您需要在源站放行DDoS高防回源IP，避免由高防转发回源站的流量被误拦截。

如果不存在上述情况，请跳过该步骤。

b. 更换源站ECS公网IP：

如果您的源站是阿里云ECS服务器，且源站IP地址不慎暴露，您需要更换ECS云服务器的公网IP，防止黑客绕过DDoS高防直接攻击源站。

如果不存在上述情况，请跳过该步骤。

c. 上传HTTPS证书：

如果接入高防的网站有HTTPS业务，您必须将域名关联的HTTPS证书上传到DDoS高防实例中配置的对应域名，才能保证HTTPS协议请求被正常响应。

> **说明** 如果网站已关联增强型DDoS高防实例，则在成功上传HTTPS证书后，您还可以为网站自定义TLS安全策略。具体操作，请参见自定义TLS安全策略。

如果网站只有HTTP业务，请跳过该步骤。

d. （可选）本地验证转发配置生效：

在本地计算机上验证添加到高防的网站配置已经生效，避免在网站配置未生效时将业务流量切换到高防，导致业务中断。

e. 修改域名的解析设置：

添加网站配置后，DDoS高防为网站分配一个CNAME地址，您必须将网站域名的DNS解析指向高防CNAME地址，才可以正式将业务流量切换到高防实例进行防护。您可以手动修改网站域名的DNS解析或者使用NS接入的方式自动修改DNS解析。

相关操作，请参见手动修改DNS解析接入网站业务、NS方式接入网站业务。

iii. 单击**去网站列表**，您可以在网站列表中查看新添加的网站域名和域名对应的高防CNAME地址。

完成**添加网站**配置向导后，您可以对已经添加的网站配置执行以下操作：


- 添加备注：单击**备注**后的

  图标，为该网站配置添加备注信息，便于后续识别。

- **编辑**、**删除**：编辑、删除已添加的网站配置。

  > **注意** 您可以通过编辑网站配置，开启高防流量标记功能，使DDoS高防在回源请求的自定义Header字段记录特定的信息。该功能可用于获取客户端真实源端口、记录高防转发流量等场景。更多信息，请参见设置流量标记。

- **DNS设置**：如果您开启了付费版的阿里云云解析DNS服务，则可以使用NS接入方式自动修改域名DNS，完成业务流量切换到高防进行防护。

  具体操作，请参见NS方式接入网站业务。

- **防护设置**：前往**网站业务DDoS防护**页签，修改网站的DDoS防护功能配置。

  成功添加网站配置后，DDoS高防默认为网站开启**AI智能防护**和**频率控制**防护功能，您可以在**网站业务DDoS防护**页签，为网站开启更多的防护功能和修改防护功能的规则。

  具体操作，请参见设置AI智能防护。

- **回源设置**：如果接入高防的网站有多个源站服务器，您可以通过回源设置修改**回源负载算法**。

  具体操作，请参见修改回源设置。

## 执行结果

DDoS高防为已接入的网站业务分配一个CNAME地址。您只需将网站域名的DNS解析指向DDoS高防的CNAME地址，即可将网站访问流量转发到DDoS高防实例进行清洗。

## 后续步骤

- 步骤2：接入网站业务流量
- （可选）上传HTTPS证书：若您的网站支持HTTPS协议，您必须上传HTTPS证书，才能使DDoS高防正常清洗HTTPS业务流量。

# 2.1.3. 步骤2：接入网站业务流量

通过DDoS高防域名接入添加网站业务后，您需要更新域名的DNS解析，将网站业务流量解析到DDoS高防。完成切换后，网站的访问流量都会先经过DDoS高防清洗，再转发到源站服务器。本文以网站域名解析托管在阿里云云解析DNS为例，介绍了更新域名解析CNAME记录以接入DDoS高防的操作方法。

## 前提条件

- 已完成域名接入。具体操作，请参见步骤1：添加网站业务转发规则。
- 源站服务器已放行DDoS高防回源IP。如果您的源站服务器上部署了非阿里云安全软件（例如，第三方防火墙），请将DDoS高防的回源IP地址加入安全软件的白名单，避免DDoS高防的回源流量被源站服务器上的安全软件误拦截。更多信息，请参见放行DDoS高防回源IP。
- 验证转发配置生效。强烈建议您在切换网站访问流量前，在本地验证DDoS高防实例的业务转发配置已经生效。更多信息，请参见本地验证转发配置生效。

> **警告** 如果转发配置未生效就执行业务切换，将可能导致业务中断。

## 背景信息

以下操作描述建立在您的域名DNS托管在阿里云云解析DNS的前提下。

> **说明** 云解析DNS是阿里云提供的域名解析服务，支持免费的公共DNS服务和付费版增值服务。如果您的域名已开通付费版云解析DNS服务，我们推荐您使用NS接入（即自动修改DNS）的方式接入DDoS高防。更多信息，请参见NS方式接入网站业务。

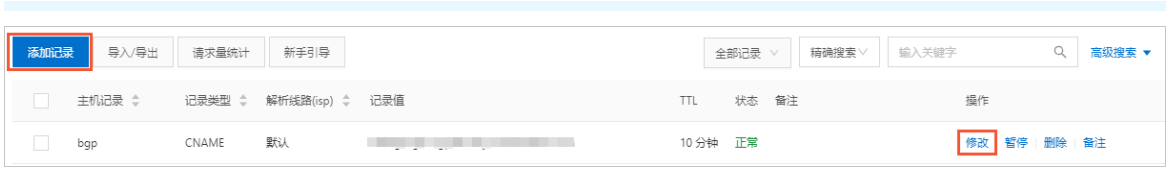
如果您使用其他DNS服务商的域名解析服务，请登录服务商系统修改网站域名的解析记录，下文内容仅供参考。

假设在DDoS高防控制台已添加网站的域名为 `bgp.aliyundoc.com` 。以下操作示例描述了在云解析DNS控制台修改、新增域名解析的步骤。

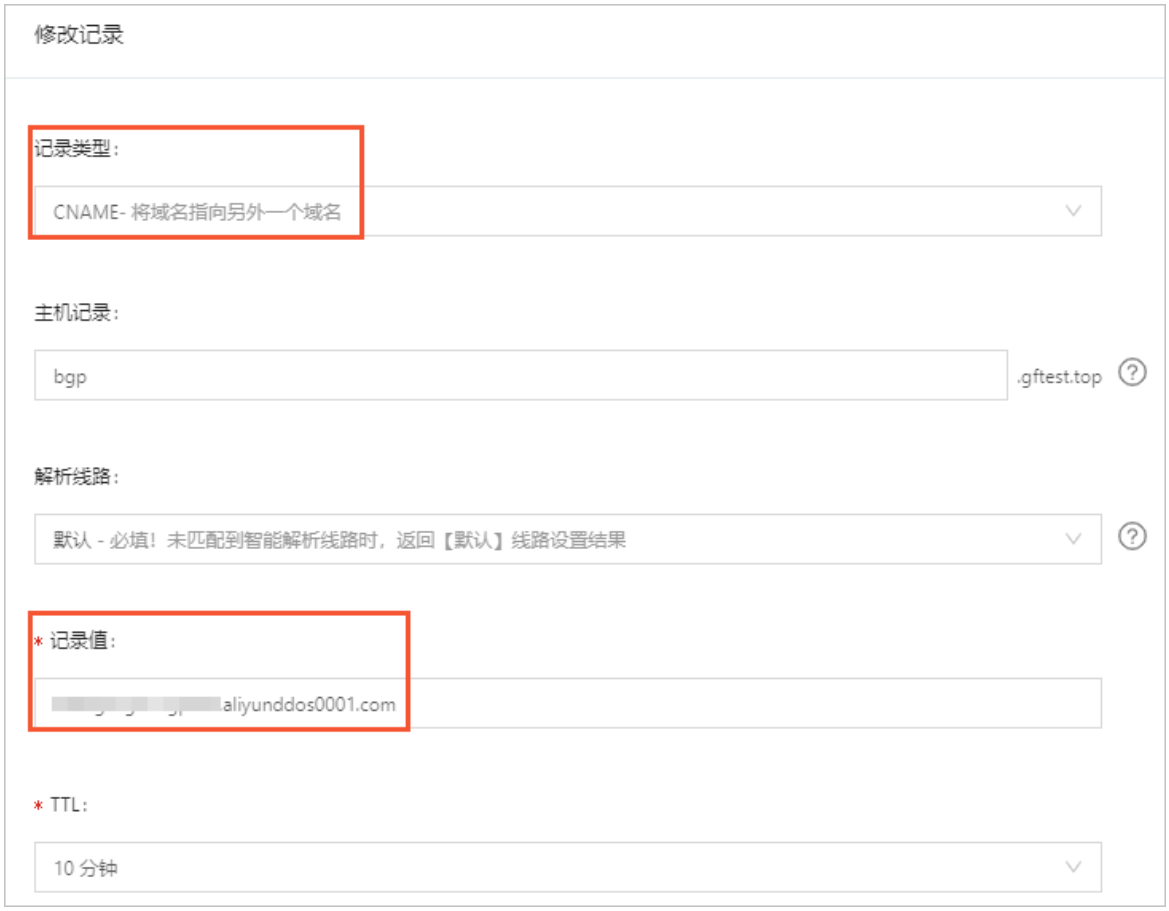
## 操作步骤

1. 登录阿里云云解析DNS控制台。
2. 在**域名解析**页面，定位到要操作的域名（本示例中为 `aliyundoc.com` ），单击**操作**列下的**解析设置**。
3. 在**解析设置**页面，定位到要修改的解析记录（本示例中对应主机记录为**bgp**的A记录或CNAME记录），单击**操作**列下的**修改**。

> **说明** 如果要操作的解析记录不在记录列表中，您可以单击**添加记录**。




4. 在**修改记录**（或**添加记录**）对话框，选择**记录类型**为**CNAME**，并将**记录值**修改为域名的DDoS高防CNAME地址。




5. 单击**确认**，等待修改后的解析设置生效。

## 后续步骤

步骤3：设置网站业务防护策略

# 2.1.4. 步骤3：设置网站业务防护策略

网站业务接入DDoS高防后，默认启用AI智能防护，无需您进行额外操作。在遇到异常情况或有特殊需求时，您可以手动调整网站业务的DDoS防护策略，具体包括AI智能防护、针对域名的黑白名单、针对域名的区域封禁、精确访问控制、频率控制。

## 前提条件

已完成域名接入。更多信息，请参见步骤1：添加网站业务转发规则。

## 操作步骤

1. 登录DDoS高防控制台。

2. 在顶部菜单栏左上角处，选择服务所在地域：
   - **中国内地**：选择该地域将跳转到**DDoS高防（新BGP）**控制台。
   - **非中国内地**：选择该地域将跳转到**DDoS高防（国际）**控制台。

     您可以通过切换地域分别管理和配置DDoS高防（新BGP）和DDoS高防（国际）实例。在使用DDoS高防服务时，请确认您已选择正确的地域。
3. 在左侧导航栏，选择**接入管理 > 域名接入**。
4. 在**域名接入**页面，定位到要操作的域名，单击其操作列下的**防护设置**。


5. 在**网站业务DDoS防护**页签，根据需要为目标域名设置DDoS防护策略。支持设置的DDoS防护策略包括AI智能防护、针对域名的黑白名单、针对域名的区域封禁、精确访问控制、频率控制。


   - **AI智能防护**：默认开启。由智能大数据分析引擎自学习业务流量基线，发现并阻断新型CC攻击，在流量异常时，基于历史流量分布，动态调整各执行模块策略阻断异常请求。支持手动修改防护模式和等级。更多信息，请参见设置AI智能防护。
   - **黑白名单（针对域名）**：开启针对域名的访问源IP黑白名单后，黑名单IP/IP段对域名的访问请求将会被直接阻断，白名单IP/IP段对域名的访问请求将被直接放行，且不经过任何防护策略过滤。更多信息，请参见设置黑白名单（针对域名）。
   - **区域封禁（针对域名）**：开启针对域名的区域封禁后，您可以一键阻断来自指定地区（中国大陆省/市/区、非中国大陆地区）来源IP的所有网站访问请求。更多信息，请参见设置区域封禁（针对域名）。
   - **精确访问控制**：开启精确访问控制后，您可以使用常见的HTTP字段（例如IP、URL、Referer、UA、参数等）设置匹配条件，用来筛选访问请求，并对命中条件的请求设置放行、封禁、挑战操作。更多信息，请参见设置精准访问控制。
   - **频率控制**：开启频率控制后，您可以限制单一源IP对网站的访问频率。频率控制开启后自动生效，且

默认使用正常防护模式，帮助网站防御一般的CC攻击。支持手动调整防护模式和自定义访问频率控制规则。更多信息，请参见设置频率控制。

# 2.1.5. 步骤4：查看网站业务防护数据

网站业务接入DDoS高防后，您可以在DDoS高防控制台使用安全总览和日志功能查看业务防护数据。

## 前提条件

- 已完成域名接入。更多信息，请参见步骤1：添加网站业务转发规则。
- 已完成业务流量接入配置。更多信息，请参见步骤2：接入网站业务流量。

## 操作步骤

1. 登录DDoS高防控制台。
2. 在顶部菜单栏左上角处，选择服务所在地域：
   - **中国内地**：选择该地域将跳转到**DDoS高防（新BGP）**控制台。
   - **非中国内地**：选择该地域将跳转到**DDoS高防（国际）**控制台。

     您可以通过切换地域分别管理和配置DDoS高防（新BGP）和DDoS高防（国际）实例。在使用DDoS高防服务时，请确认您已选择正确的地域。
3. 查看安全总览。
   i. 在左侧导航栏，单击**安全总览**。
   ii. 单击**域名**页签，选择要查询的域名和时间范围，查看防护总览数据。


更多信息，请参见查看安全总览。

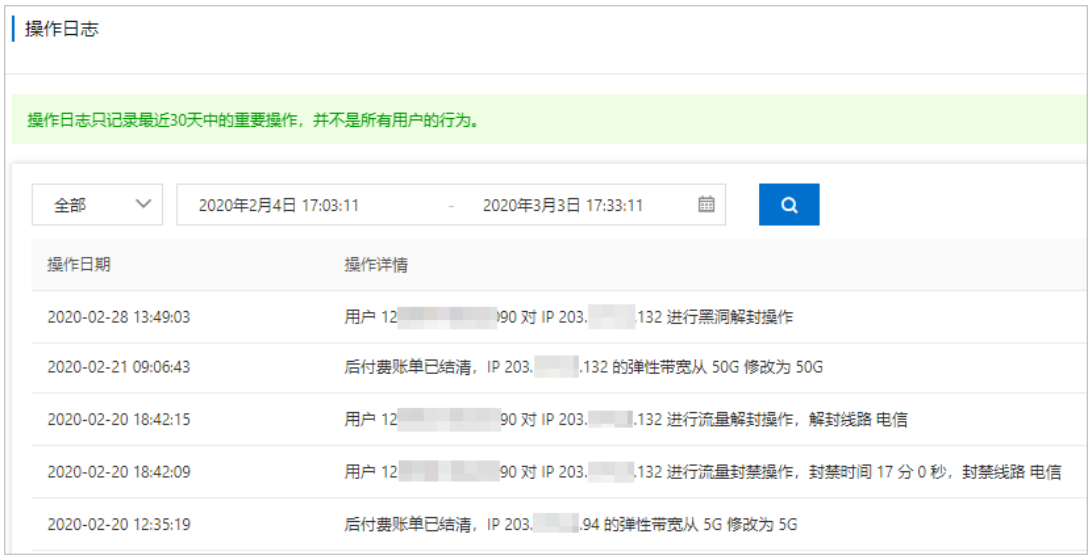
4. 查询和分析日志。
   - 查询操作日志

> **说明** 仅DDoS高防（新BGP）支持操作日志功能。如果您使用DDoS高防（国际），则推荐您开通全量日志分析。

操作日志记录了最近30天中的重要操作，例如IP、ECS实例操作等。

a. 在左侧导航栏，单击**调查分析 > 操作日志**。

b. 在**操作日志**页面，选择要查询的操作对象和时间范围，查看操作日志记录。




更多信息，请参见查询操作日志。

- 查询全量日志

如果您希望对DDoS高防的日志进行实时分析和报表展示，推荐您开通DDoS高防全量日志分析。开通全量日志分析后，阿里云日志服务将对接DDoS高防的网站访问日志和CC攻击日志，并对采集到的日志数据进行实时检索与分析，以仪表盘形式向您展示查询结果。更多信息，请参见什么是日志服务。

DDoS高防全量日志分析是增值服务，需要单独开通并启用。要使用全量日志分析，您需要完成以下任务：

a. 开通全量日志分析，具体操作请参见开通全量日志。

b. 启用全量日志功能，具体操作请参见为网站启用全量日志。

开通并启用全量日志功能后，您可以在**调查分析 > 全量日志分析**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。

> **说明** 关于全量日志中记录的字段，请参见全量日志字段说明。

更多信息，请参见概述。

# 2.2. 防护非网站业务

## 2.2.1. 概览

本文将指导您在开通DDoS高防后，快速部署和使用DDoS高防，为您的非网站业务（例如端游、手游、app等）配置DDoS防护。

使用DDoS高防防护非网站业务时，您可以按照以下步骤进行操作。

| 任务名 | 描述 |
| --- | --- |
| 步骤1：添加端口转发规则 | 在DDoS高防控制台通过端口接入添加要防护的非网站业务，并使用DDoS高防IP作为您的业务IP，将业务流量牵引到DDoS高防实例。完成切换后，业务流量都会先经过DDoS高防清洗，再转发到源站服务器。 |
| 步骤2：设置端口转发和防护策略 | 在DDoS高防实例下添加端口转发规则后，您可以根据需要设置端口转发策略，例如会话保持、（多源站IP）健康检查，也可以为非网站业务设置DDoS防护策略，例如虚假源检测、目的限速、包长度过滤、源限速。 |
| 步骤3：查看端口防护数据 | 非网站业务接入DDoS高防后，您可以在DDoS高防的安全总览页面查看端口流量转发数据。 |

## 2.2.2. 步骤1：添加端口转发规则

使用DDoS高防防护非网站业务（例如，端游、手游、App等）时，您必须在购买DDoS高防实例后，配置端口转发规则，然后使用DDoS高防IP作为您的业务IP，实现业务接入。本文介绍了在DDoS高防控制台配置端口转发规则的具体操作。

### 前提条件

已购买DDoS高防（新BGP）或DDoS高防（国际）实例。更多信息，请参见购买DDoS高防实例。

### 背景信息

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（例如，CC攻击、Web攻击防护等），只支持四层防护（例如，防护SYN Flood、UDP Flood等）。接入非网站业务时，您只需配置DDoS高防实例的端口转发规则，然后使用DDoS高防IP作为业务IP即可。

### 操作步骤

1. 登录DDoS高防控制台。
2. 在顶部菜单栏左上角处，选择服务所在地域：
   - **中国内地**：选择该地域将跳转到**DDoS高防（新BGP）**控制台。
   - **非中国内地**：选择该地域将跳转到**DDoS高防（国际）**控制台。

     您可以通过切换地域分别管理和配置DDoS高防（新BGP）和DDoS高防（国际）实例。在使用DDoS高防服务时，请确认您已选择正确的地域。
3. 在左侧导航栏，选择**接入管理 > 端口接入**。
4. 在**端口接入**页面，选择要使用的DDoS高防实例，并单击**添加规则**。

> **说明** 您也可以使用批量操作添加规则，支持一次添加多条规则。更多信息，请参见批量添加规则。

5. 在**添加规则**对话框，根据您的实际业务情况完成规则配置。


| 参数 | 说明 |
| --- | --- |
| **转发协议** | 转发协议类型，可选值：**TCP**、**UDP**。 |
| **转发端口** | DDoS高防实例使用的转发端口。<br>○ 为了便于管理，建议您将**转发端口**与**源站端口**保持一致。<br>○ 根据中国国家监管政策要求，为了防止未通过备案的域名业务接入防护，DDoS高防不支持80、8080、443、8443端口的端口接入配置。关于上述接口的防护，建议您使用域名接入。更多信息，请参见添加网站。<br>○ 为了防止私自搭建DNS防护服务器，DDoS高防不支持53端口的端口接入配置。<br>○ 不允许使用已配置的转发端口。同一DDoS高防实例（IP）和转发协议下，转发规则的转发端口必须唯一。当您尝试添加同协议-同转发端口的规则时，系统将提示转发规则冲突。请注意不要与通过网站配置自动生成的转发规则冲突。更多信息，请参见（添加网站）自动生成转发规则。 |
| **源站端口** | 源站使用的业务端口。 |
| **源站IP** | 源站的IP地址。<br>**说明** 支持添加多个源站IP以实现自动负载均衡。多个IP间以半角逗号（,）分隔。最多可配置20个源站IP。 |

6. 单击**确定**。

## 后续步骤

端口转发规则创建完成后，您还需要将要防护的实际业务IP替换为DDoS高防IP，才能正式将业务流量切换到DDoS高防。完成切换后，业务流量都会先经过DDoS高防清洗，再转发到源站服务器。

> **注意** 强烈建议您在正式切换业务流量前进行验证，确认转发配置已生效。关于转发配置的验证方法，请参见本地验证转发配置生效。如果转发配置未生效就执行业务切换，将可能导致业务中断。

完成业务流量切换后，DDoS高防使用默认策略帮助您清洗和转发流量。您可以根据业务需要，自定义DDoS防护策略和开启会话保持、健康检查功能。具体操作，请参见步骤2：设置端口转发和防护策略。

# 2.2.3. 步骤2：设置端口转发和防护策略

在DDoS高防实例下添加端口转发规则后，您可以根据需要配置端口转发策略，例如会话保持、（多源站IP）健康检查，也可以为非网站业务设置DDoS防护策略，例如虚假源检测、目的限速、包长度过滤、源限速。

## 前提条件

已完成端口接入。更多信息，请参见步骤1：添加端口转发规则。

## 背景信息

通过设置端口转发策略和非网站业务DDoS防护策略，您可以根据业务实际需求，优化DDoS高防的转发功能。

支持的设置功能包括：

- 开启基于IP地址的会话保持，可以将来自同一IP地址的请求转发到同一个后端服务器。
- 开启健康检查，可以检测后端服务器的可用性，在转发客户端请求时避开异常服务器。
- 开启DDoS防护策略，可以对接入DDoS高防的非网站业务的连接速度、包长度等参数进行限制，缓解小流量的连接型攻击。

## 操作步骤

1. 登录DDoS高防控制台。
2. 在顶部菜单栏左上角处，选择服务所在地域：
   - **中国内地**：选择该地域将跳转到**DDoS高防（新BGP）**控制台。
   - **非中国内地**：选择该地域将跳转到**DDoS高防（国际）**控制台。

     您可以通过切换地域分别管理和配置DDoS高防（新BGP）和DDoS高防（国际）实例。在使用DDoS高防服务时，请确认您已选择正确的地域。
3. 在左侧导航栏，选择**接入管理 > 端口接入**。
4. 在**端口接入**页面，选择DDoS高防实例，并定位到要操作的转发规则，根据需要设置会话保持、健康检查、非网站业务DDoS防护策略。


   - **会话保持**
     a. 单击**会话保持**列下的**配置**

a. 单击**会话保持**列下的**配置**。

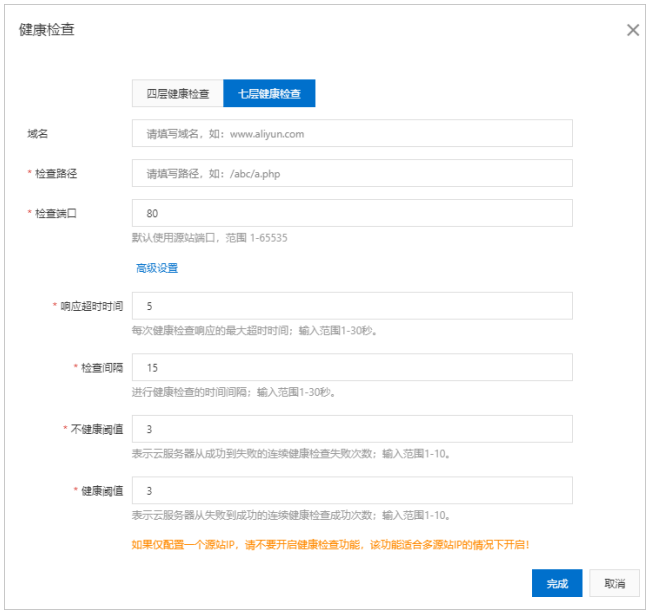
b. 在**会话保持**对话框，根据需要开启或关闭会话保持。


- 开启会话保持：设置**超时时间**，并单击**设置超时时间并开启**。
- 关闭会话保持：单击**关闭会话保持**。

- **健康检查**

a. 单击**健康检查**列下的**配置**。

b. 在**健康检查**对话框，完成健康检查配置。关于配置参数的描述，请参见健康检查配置项说明。




c. 单击**完成**。

开启健康检查后，如果您想关闭健康检查，只需单击**配置**，并在**健康检查**对话框单击**关闭健康检查**。

- 非网站业务DDoS防护策略

a. 单击**DDoS防护策略**列下的**配置**。

b. 在**非网站业务DDos防护**页签，根据需要为当前转发规则设置DDoS防护策略，包括虚假源、目的限速、包长度过滤、源限速。


- **虚假源**：针对虚假IP发起的DDoS攻击进行校验过滤。
- **目的限速**：以当前高防IP、端口为统计对象，当每秒访问频率超出阈值时，对当前高防IP的端口进行限速，其余端口不受限速影响。
- **包长度过滤**：设置允许通过的包最小和最大长度，小于最小长度或者大于最大长度的包会被丢弃。
- **源限速**：以当前高防IP、端口为统计对象，对访问频率超出阈值的源IP地址进行限速。访问速率未超出阈值的源IP地址，访问不受影响。源限速支持黑名单控制，对于60秒内5次超限的源IP，您可以启用将源IP加入黑名单的策略，并设置黑名单的有效时长。

更多信息，请参见设置DDoS防护策略。

## 后续步骤

步骤3：查看端口防护数据

# 2.2.4. 步骤3：查看端口防护数据

非网站业务接入DDoS高防后，您可以在DDoS高防的安全总览页面查看端口流量转发数据。

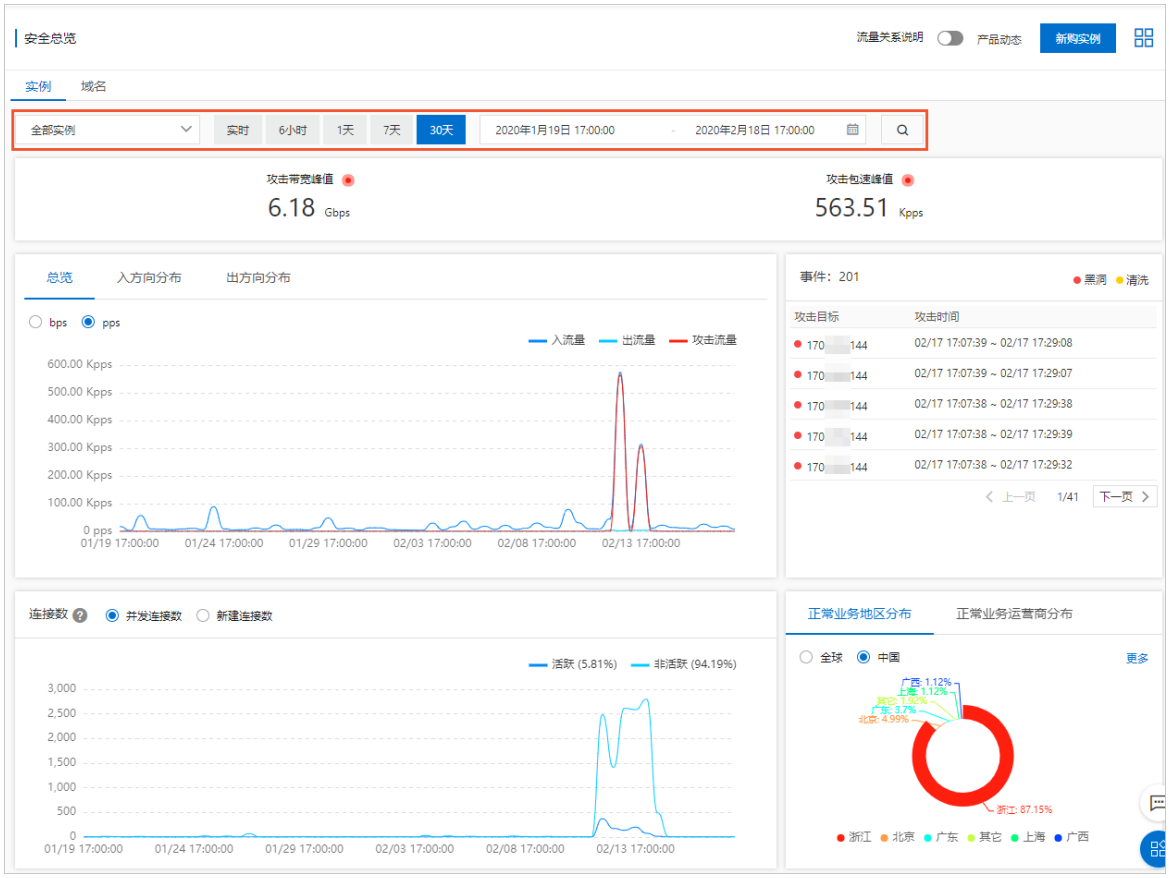
## 前提条件

已完成端口接入。更多信息，请参见步骤1：添加端口转发规则。

## 操作步骤

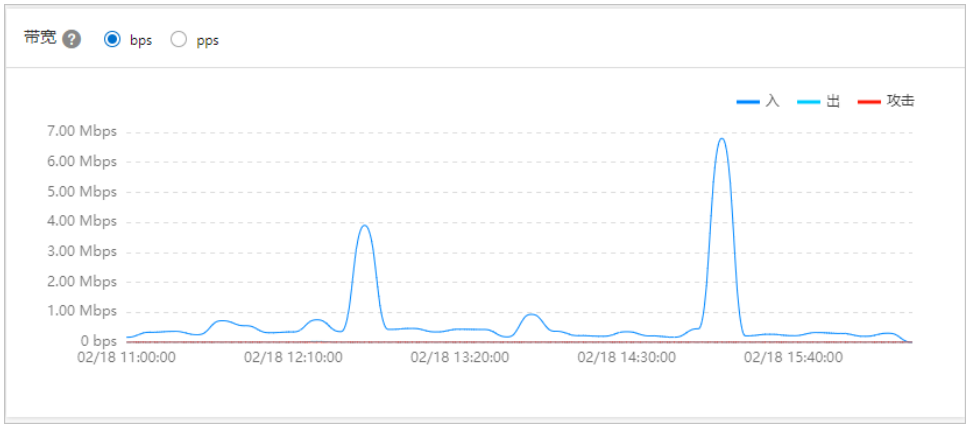
1. 登录DDoS高防控制台。
2. 在顶部菜单栏左上角处，选择服务所在地域：
   - **中国内地**：选择该地域将跳转到**DDoS高防（新BGP）**控制台。
   - **非中国内地**：选择该地域将跳转到**DDoS高防（国际）**控制台。

     您可以通过切换地域分别管理和配置DDoS高防（新BGP）和DDoS高防（国际）实例。在使用DDoS高防服务时，请确认您已选择正确的地域。
3. 在左侧导航栏，单击**安全总览**。
4. 单击**实例**页签，设置要查询的实例和时间范围，查看指定实例对应业务的相关信息。

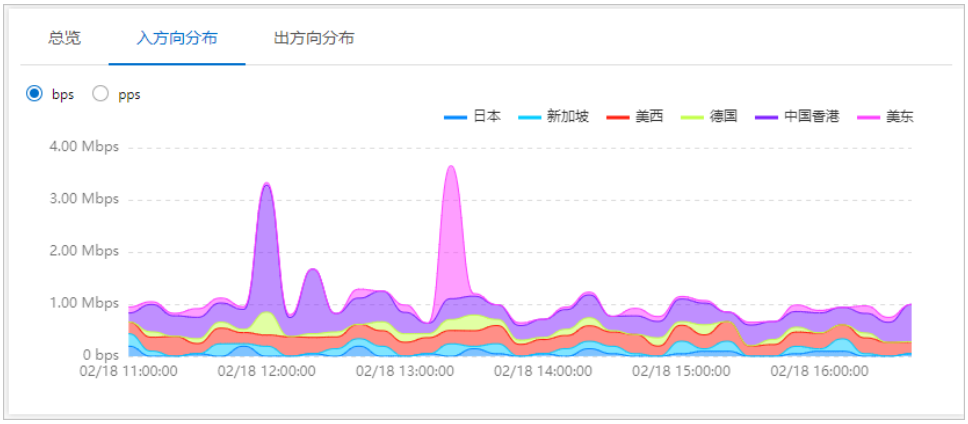



支持查看的实例业务信息包括以下内容：

- **攻击带宽峰值**（单位：bps）和**攻击包速峰值**（单位：pps）
- 流量趋势信息
  - DDoS高防（新BGP）服务提供**带宽**趋势图，以**bps**或者**pps**展示指定时间段内实例上的入流量、出流量、攻击流量趋势。

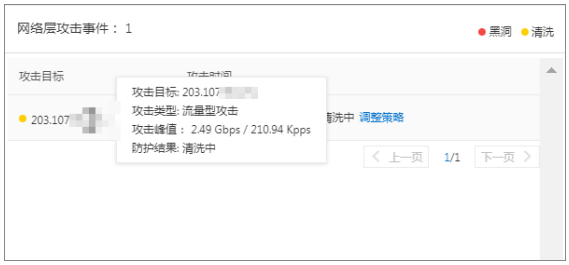


- DDoS高防（国际）提供三个页签，分别是**总览**（与带宽趋势图相同）、**入方向分布**（入方向流量的分布信息）、**出方向分布**（出方向流量的分布信息）。



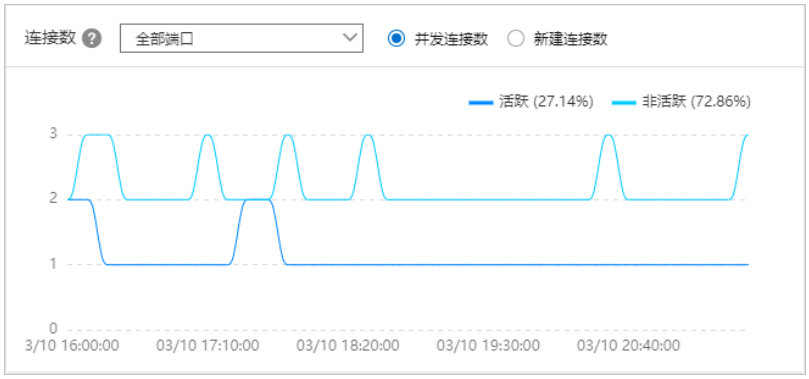

- **（黑洞和清洗）网络层攻击事件**

  将光标放置在被攻击的IP或端口上，可以展示被攻击的IP和端口信息、攻击的类型和峰值、防护结果。



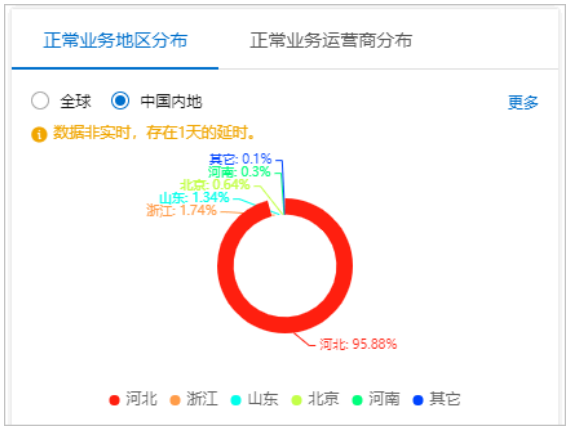

- **（端口）连接数**
  - **并发连接数**：客户端同一时间与DDoS高防建立的TCP连接数量。
  - **新建连接数**：客户端每秒内新增的与DDoS高防通信的TCP连接数。
  - **活跃连接数**：当前所有状态为Established的TCP连接数量。
  - **非活跃连接数**：当前除了Established状态以外，所有其他状态的TCP连接数量。

> **说明** 只有选择单个实例时，连接数报表处才会显示当前实例IP的不同端口的连接数。如果选择一个以上实例，则无法区别端口，只能显示全部端口的连接数。




- **正常业务地区分布**和**正常业务运营商分布**
  - **正常业务地区分布**：正常业务流量的来源地区（**全球**、**中国内地**）分布

- **正常业务运营商分布**：正常业务流量的运营商分布



# 3.查看安全总览

业务接入DDoS高防并切换业务流量至DDoS高防实例后，您可以在DDoS高防控制台的安全总览页面实时查看业务指标和DDoS攻击事件的防护情况。

## 前提条件

已创建DDoS高防（新BGP或国际）实例并完成业务接入。更多信息，请参见以下文档：

- 购买DDoS高防实例
- （防护网站业务）添加网站
- （防护非网站业务）添加规则

## 背景信息

DDoS高防的安全总览页面向您展示以下业务指标和DDoS攻击事件的概览：

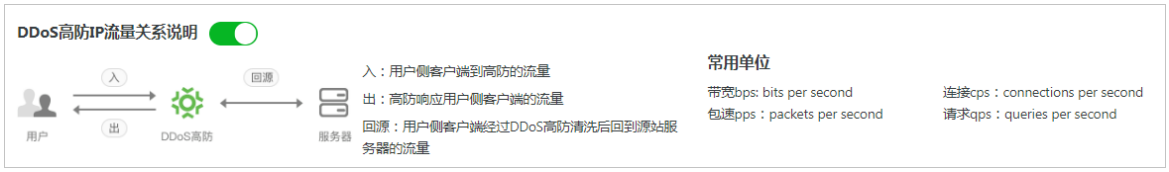
- 业务指标：业务带宽、业务QPS、业务CPS、接入防护的域名、接入防护的端口。
- DDoS攻击事件：流量型、连接型和Web资源消耗型三种DDoS攻击事件的记录。

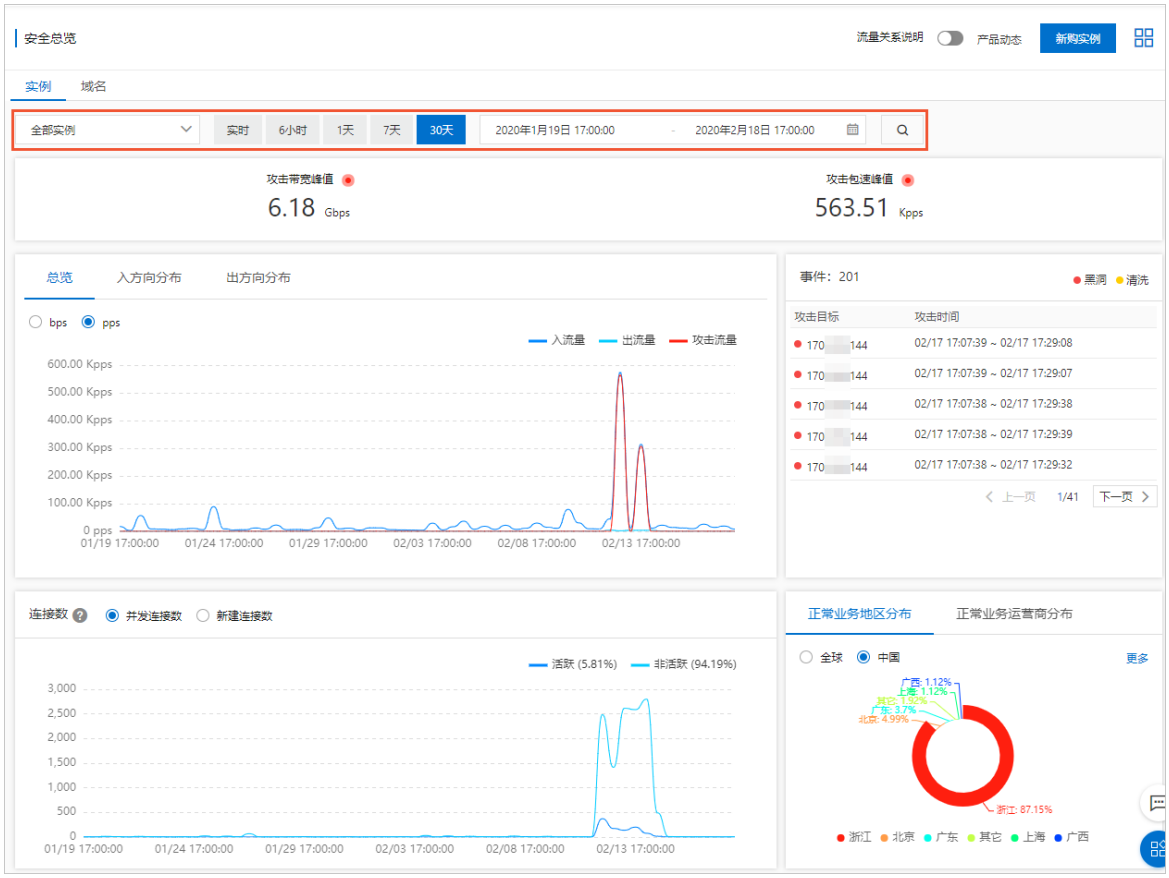
## 操作步骤

1. 登录DDoS高防控制台。
2. 在顶部菜单栏左上角处，选择服务所在地域：
   - **中国内地**：选择该地域将跳转到**DDoS高防（新BGP）**控制台。
   - **非中国内地**：选择该地域将跳转到**DDoS高防（国际）**控制台。

     您可以通过切换地域分别管理和配置DDoS高防（新BGP）和DDoS高防（国际）实例。在使用DDoS高防服务时，请确认您已选择正确的地域。
3. 在左侧导航栏，单击**安全总览**。
4. （可选）展开**流量关系说明**，查看并熟悉DDoS高防IP的背景信息及相关概念。

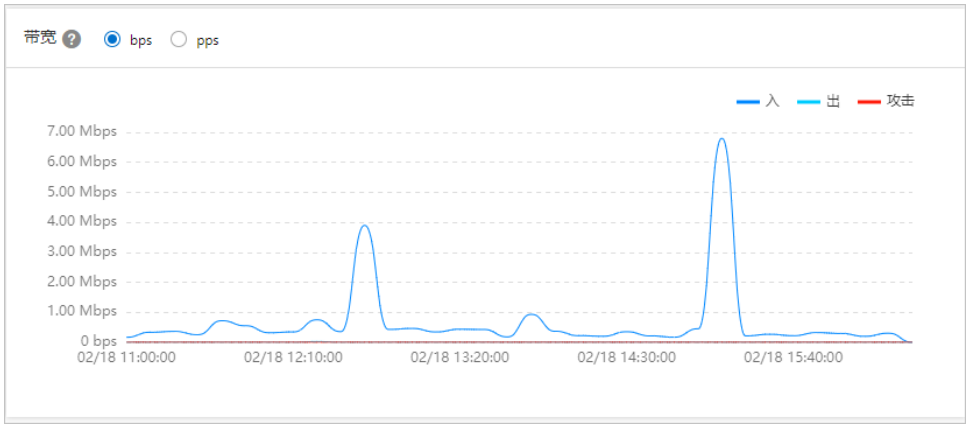
   **DDoS高防IP流量关系说明**展示了DDoS高防IP的流量关系说明、高防数据指标的名词解释和常用数据单位。

   
   
5. 单击**实例**页签，设置要查询的实例和时间范围，查看指定实例对应业务的相关信息。

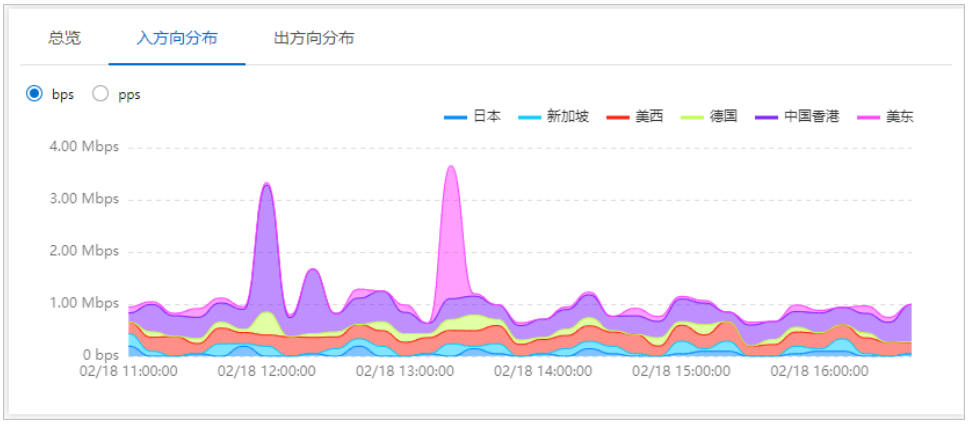



支持查看的实例业务信息包括以下内容：

- **攻击带宽峰值**（单位：bps）和**攻击包速峰值**（单位：pps）
- 流量趋势信息
  - DDoS高防（新BGP）服务提供**带宽**趋势图，以**bps**或者**pps**展示指定时间段内实例上的入流量、出流量、攻击流量趋势。

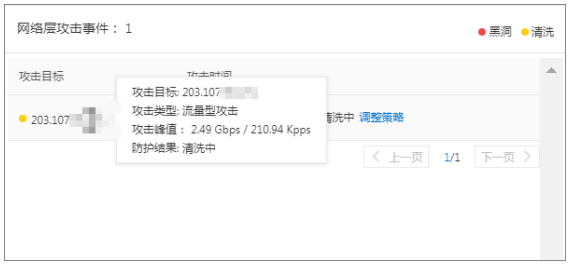


- DDoS高防（国际）提供三个页签，分别是**总览**（与带宽趋势图相同）、**入方向分布**（入方向流量的分布信息）、**出方向分布**（出方向流量的分布信息）。



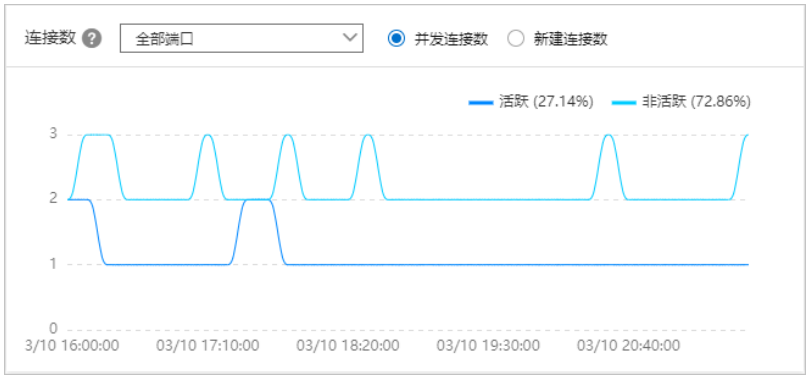

- （黑洞和清洗）**网络层攻击事件**

  将光标放置在被攻击的IP或端口上，可以展示被攻击的IP和端口信息、攻击的类型和峰值、防护结果。



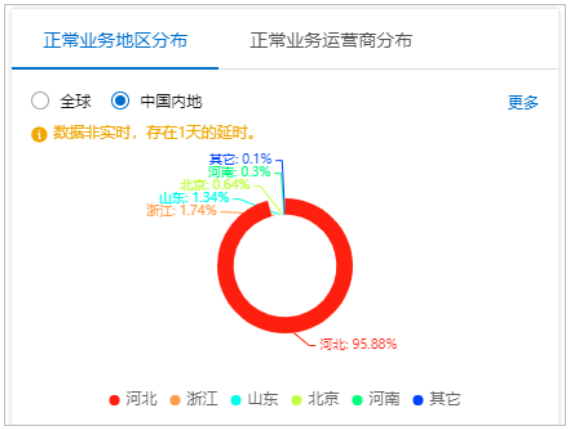

- （端口）**连接数**
  - **并发连接数**：客户端同一时间与DDoS高防建立的TCP连接数量。
  - **新建连接数**：客户端每秒内新增的与DDoS高防通信的TCP连接数。
  - **活跃连接数**：当前所有状态为Established的TCP连接数量。
  - **非活跃连接数**：当前除了Established状态以外，所有其他状态的TCP连接数量。

> **说明** 只有选择单个实例时，连接数报表处才会显示当前实例IP的不同端口的连接数。如果选择一个以上实例，则无法区别端口，只能显示全部端口的连接数。




- **正常业务地区分布**和**正常业务运营商分布**
  - **正常业务地区分布**：正常业务流量的来源地区（**全球**、**中国内地**）分布

- **正常业务运营商分布**：正常业务流量的运营商分布




6. 单击**域名**页签，设置要查询的时间范围，查看指定域名对应业务的相关信息。


支持查看的域名业务信息包括以下内容：

- **HTTP清洗峰值**（单位：QPS）和**HTTPS清洗峰值**（单位：QPS）
- **请求速率（QPS）**趋势图

  请求速率趋势图按峰值展示，不同的查询时间间隔对应的展示粒度不同，具体如下：

  - 1小时以内：展示粒度为1分钟。
  - 1~6小时以内：展示粒度为10分钟。
  - 6~24小时：展示粒度为30分钟。
  - 1~7天：展示粒度为1小时。
  - 7~15天：展示粒度为4小时。
  - 其他：展示粒度为12小时。

- **应用层清洗事件**

  将光标放置在域名上，可以展示被攻击的域名信息、攻击的峰值和攻击类型。

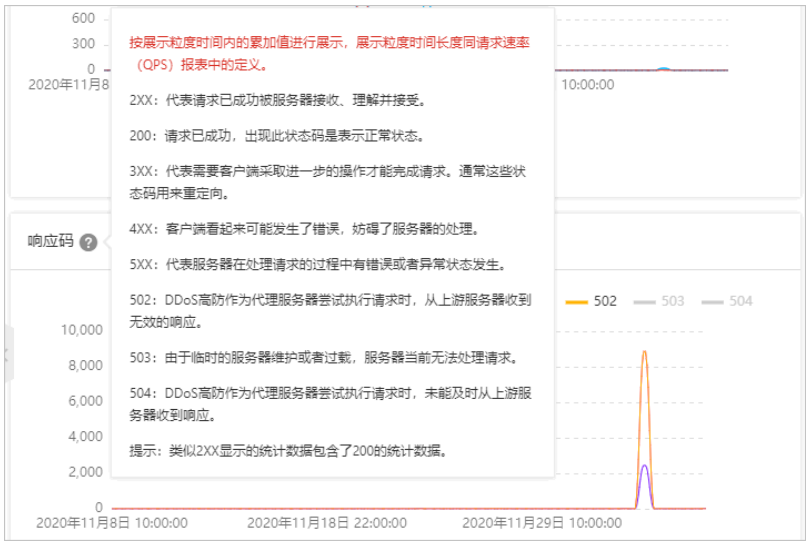
- **响应码**趋势图

  响应码记录的数量对应展示粒度时间内的累加值。关于展示粒度的时间长度定义，请参见**请求速率（QPS）**趋势图中的说明。不同响应码的含义如下：

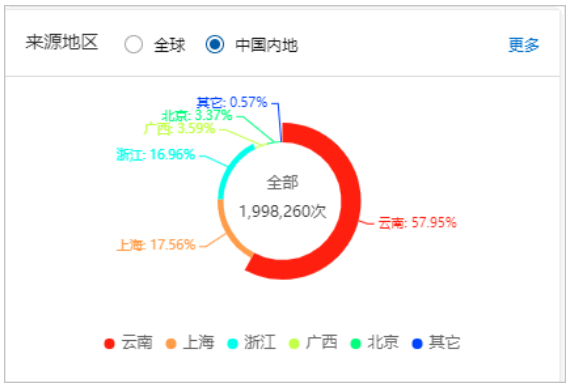
  - 2XX：表示请求已成功被服务器接收、理解并接受。

    > **说明** 2XX响应码的统计数据包含了200响应码的统计数据。

  - 200：表示请求成功。
  - 3XX：表示需要客户端采取进一步的操作才能完成请求。通常这些状态码用来重定向。
  - 4XX：表示客户端可能发生了错误，妨碍服务器的处理。
  - 5XX：表示服务器在处理请求的过程中发生了错误或者出现异常状态。
  - 502：表示DDoS高防作为代理服务器尝试执行请求，但是从上游服务器收到了无效的响应。
  - 503：表示服务器当前无法处理请求，可能因为临时的服务器维护或者过载。
  - 504：表示DDoS高防作为代理服务器尝试执行请求，但是未能及时从上游服务器收到响应。

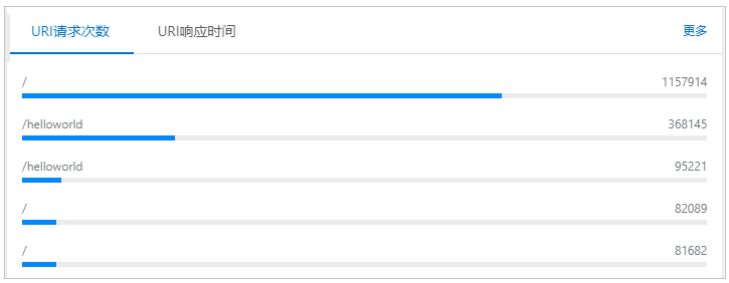



- 访问**来源地区**分布：访问来源地区（**全球**、**中国内地**）的分布



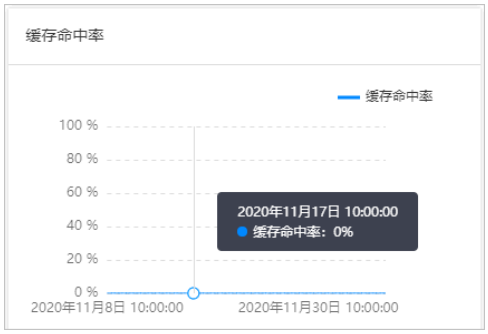

- **URI请求次数**和**URI响应时间**记录
  - **URI请求次数**：按被请求次数由多到少返回前五个URI（单击**更多**可以查看全部URI的请求次数）

- **URI响应时间**：按响应时间（单位：秒）由大到小返回前五个URI（单击**更多**可以查看全部URI的响应时间）




- **缓存命中率**趋势图

  适用于已经开启静态页面缓存功能的场景。更多信息，请参见设置静态页面缓存。



# 4.接入管理

# 4.1. 域名接入

## 4.1.1. 添加网站

网站业务接入DDoS高防时，您必须在DDoS高防控制台添加一条网站配置，设置网站业务接入DDoS高防后的流量转发信息。网站配置支持批量操作。本文介绍了添加网站配置和批量导入网站配置的操作步骤。

### 前提条件

- 已购买DDoS高防（新BGP）或DDoS高防（国际）实例。

  相关操作，请参见购买DDoS高防实例。

- 如果网站业务要接入DDoS高防（新BGP）实例进行防护，则网站域名必须已经完成ICP备案。如果网站业务要接入DDoS高防（国际）实例进行防护，则网站域名无需完成ICP备案。

  关于ICP备案的更多信息，请参见ICP备案流程概述。

  > **注意** 由于ICP备案有时效性，建议您在将网站业务接入DDoS高防后，仍注意维护域名的备案信息。DDoS高防会定期查询已接入防护的网站域名的备案状态。如果检测到域名备案已经失效，DDoS高防会停止相关业务的流量转发，并在**域名接入**页面为您展示如下图所示的提示。出现以下提示时，如果您需要恢复业务流量转发，必须及时更新域名的备案状态，并提交工单申请恢复流量转发。


### 添加网站配置

1. 登录DDoS高防控制台。
2. 在顶部菜单栏左上角处，选择服务所在地域：
   - **中国内地**：选择该地域将跳转到**DDoS高防（新BGP）**控制台。
   - **非中国内地**：选择该地域将跳转到**DDoS高防（国际）**控制台。

     您可以通过切换地域分别管理和配置DDoS高防（新BGP）和DDoS高防（国际）实例。在使用DDoS高防服务时，请确认您已选择正确的地域。
3. 在左侧导航栏，选择**接入管理 > 域名接入**。
4. 在**域名接入**页面，单击**添加网站**。

   您也可以批量导入网站配置。具体操作，请参见批量导入网站配置。
5. 按照页面提示，完成**添加网站**配置向导。

   i. **填写网站信息**。


填写以下网站信息，并单击**添加**。

| 参数 | 适用的实例类型 | 说明 |
| --- | --- | --- |
| **功能套餐** | DDoS高防（新BGP）和DDoS高防（国际） | 选择要关联的DDoS高防实例的功能套餐。可选项：**标准功能**、**增强功能**。<br>您可以将光标放置在**功能套餐**后的图标上，查看标准功能和增强功能套餐的功能差异（如下图所示）。 |

| 功能分类 | 功能列表 | 标准功能 | 增强功能 |
| --- | --- | --- | --- |
| 防护算法 | 流量型攻击防护 | ✓ | ✓ |
| | 资源耗尽型攻击防护（四七层CC攻击防护） | ✓ | ✓ |
| | AI智能防护 | ✓ | ✓ |
| 防护规则 | 黑白名单 | ✓ | ✓ |
| | 精准访问控制 | 5条<br>支持部分匹配字段 | 10条 |
| | 区域IP封禁 | × | ✓ |
| 业务接入 | HTTP（80/8080），HTTPS（443/8443）转发 | ✓ | ✓ |
| | HTTP，HTTPS非标端口转发 | × | 10个端口 |
| | TLS协议加密套件自定义 | × | ✓ |
| | HTTP 2.0、HTTPS跳转、HTTP回源和回源负载策略 | ✓ | ✓ |
| 其他 | 静态页面缓存 | × | ✓ |

| 参数 | 适用的实例类型 | 说明 |
| --- | --- | --- |
| **实例** | DDoS高防（新BGP）和DDoS高防（国际） | 选择要关联的DDoS高防实例。一个网站域名最多可以关联8个DDoS高防实例，且只能关联同一种**功能套餐**下的多个实例。<br>此处根据您选择的**功能套餐**类型显示对应的DDoS高防实例。如果无可选实例，表示您当前无可用的该功能套餐的DDoS高防实例。您可以新购实例或升级已有的标准功能套餐实例。具体操作，请参见升级实例。 |
| **网站** | DDoS高防（新BGP）和DDoS高防（国际） | 填写要防护的网站域名。具体要求如下：<br>■ 域名可以由26个英文字母（a~z、A~Z，不区分大小写）、数字（0~9）以及短划线（-）组成。域名的首位必须是字母或数字。<br>■ 支持填写泛域名，例如，`*.aliyundoc.com`。使用泛域名时，DDoS高防自动匹配该泛域名对应的子域名。<br>■ 如果同时存在泛域名和精确域名配置（例如，`*.aliyundoc.com` 和 `www.aliyundoc.com`），DDoS高防优先使用精确域名（即 `www.aliyundoc.com`）所配置的转发规则和防护策略。 |

| 参数 | 适用的实例类型 | 说明 |
| --- | --- | --- |
| **协议类型** | DDoS高防（新BGP）和DDoS高防（国际） | 选择网站支持的协议类型。可选项：<br>■ **HTTP**<br>■ **HTTPS**：如果网站支持HTTPS加密认证，请选中**HTTPS**协议，并在保存网站配置后上传网站域名使用的HTTPS证书。关于上传证书的操作，请参见上传HTTPS证书。<br>■ **Websocket**：选中该协议将自动同时选中**HTTP**协议，不支持单独选中**Websocket**协议。<br>■ **Websockets**：选中该协议将自动同时选中**HTTPS**协议，不支持单独选中**Websockets**协议。<br>选中**HTTPS**协议后，您可以根据需要开启以下高级设置：<br>  <br><br>■ **开启HTTPS的强制跳转**：适用于您的网站同时支持HTTP和HTTPS协议。开启该设置后，所有HTTP请求将被强制转换为HTTPS请求，且默认跳转到443端口。<br>**注意**<br>■ 只有当您同时选中**HTTP**和**HTTPS**协议，并且没有选中**Websocket**协议时，才可以开启该设置。<br>■ HTTP非标准端口（80以外的端口）访问的场景下，如果开启了HTTPS强制跳转，则访问默认跳转到HTTPS 443端口。<br>■ **开启HTTP回源**：适用于您的网站不支持HTTPS回源。开启该设置后，所有HTTPS协议请求将通过HTTP协议回源、所有Websockets协议请求将通过Websocket协议回源，且默认回源端口为80。<br>**注意**<br>■ 如果您的网站不支持HTTPS回源，请务必开启该设置。<br>■ HTTPS非标准端口（443以外的端口）访问的场景下，如果开启了HTTP回源，则访问默认跳转到源站HTTP 80端口。<br>■ **启用HTTP2**：开启该设置，表示源站使用了HTTP 2.0协议。 |

| 参数 | 适用的实例类型 | 说明 |
| --- | --- | --- |
| **启用OCSP** | DDoS高防（新BGP）和DDoS高防（国际） | 选择是否启用OCSP（Online Certificate Status Protocol）功能。<br><br>**注意** 该功能适用于网站HTTPS业务。如果您已选择的**协议类型**包含**HTTPS**，推荐您启用该功能。<br><br>OCSP表示在线证书状态协议，该协议用于向签发证书的CA（Certificate Authority）中心发起查询请求，检查证书是否被吊销。在与服务器进行TLS握手时，客户端必须同时获取证书和对应的OCSP响应。<br><br>OCSP功能默认未开启，表示由客户端浏览器向CA中心发起OCSP查询。该方式会导致客户端在获得OCSP响应前阻塞后续的事件，在网络情况不佳时，将造成较长时间的页面空白，降低HTTPS的性能。<br><br>启用OCSP表示由DDoS高防来执行OCSP查询并缓存查询结果（缓存时间为300秒）。当有客户端向服务器发起TLS握手请求时，DDoS高防将证书的OCSP信息随证书链一起发送给客户端，从而避免了客户端查询会产生的阻塞问题。由于OCSP响应是无法伪造的，因此这一过程不会产生额外的安全问题。 |

| 参数 | 适用的实例类型 | 说明 |
| --- | --- | --- |
| **服务器地址** | DDoS高防（新BGP）和DDoS高防（国际） | 选择源站服务器的地址类型，并填写源站服务器的地址。支持的地址类型包括：<br>■ **源站IP**：表示源站服务器的IP地址。最多支持配置20个源站IP地址，多个IP地址间使用半角逗号（,）分隔。<br>示例：<br>■ 如果源站在阿里云，一般填写源站ECS的公网IP地址；如果ECS前面部署了SLB，则填写SLB的公网IP地址。<br>■ 如果源站在阿里云外的IDC机房或者其他云服务商，您可以使用 `ping 域名` 命令，查询域名解析到的公网IP地址，并填写您获取的公网IP。<br>■ **源站域名**：通常适用于源站和高防之间还部署有其他代理服务（例如，Web应用防火墙）的场景，表示代理服务的跳转地址（例如，Web应用防火墙提供给您的CNAME地址）。最多支持配置10个源站域名，多个域名间通过换行分隔。<br>示例：如果您在部署DDoS高防实例后还需要部署Web应用防火墙（WAF），以提升应用安全防护能力，您可以选择**源站域名**类型，并填写WAF的CNAME地址。更多信息，请参见同时部署WAF和DDoS高防。<br>**注意** 如果您设置的**源站域名**为OSS存储空间（Bucket）的默认外网访问域名，则对应存储空间必须已绑定自定义域名。更多信息，请参见绑定自定义域名。<br>配置多个服务器地址（源站IP、源站域名）后，DDoS高防默认以IP Hash的方式转发网站访问流量至源站，自动实现负载均衡。保存网站配置后，您可以通过回源设置，修改源站负载算法。具体操作，请参见修改回源设置。 |

| 参数 | 适用的实例类型 | 说明 |
| --- | --- | --- |
| **服务器端口** | DDoS高防（新BGP）和DDoS高防（国际） | 根据已选择的**协议类型**，设置源站提供对应服务的端口。<br>**HTTP**协议的**服务器端口**默认为80；**HTTPS**协议的**服务器端口**默认为443。<br>**注意**<br>■ Websocket协议的端口与HTTP协议的端口一致。<br>■ Websockets和HTTP 2.0协议的端口与HTTPS协议的端口一致。<br>您可以单击**自定义**，自定义服务器端口。**HTTP**或**HTTPS**协议下均支持自定义多个端口。多个端口间使用半角逗号（,）分隔。<br>  <br>自定义服务器端口有以下要求：<br>■ 自定义端口必须在可选端口范围内。您可以单击**查看可选范围**，查看HTTP或HTTPS协议支持的可选端口范围。<br>DDoS高防实例的**功能套餐**不同，支持的可选端口范围不同，具体说明如下：<br>■ **标准功能**实例：<br>■ HTTP协议可选端口：80、8080。<br>■ HTTPS协议可选端口：443、8443。<br>■ **增强功能**实例：<br>■ HTTP协议可选端口范围：80~65535。<br>■ HTTPS协议可选端口范围：80~65535。<br>■ 所有接入DDoS高防实例防护的网站业务下自定义的不同端口（包含不同协议下的自定义端口）的总数不能超过10个。<br>示例：假设您有2个网站（A和B）要接入DDoS高防实例防护，网站A提供HTTP服务、网站B提供HTTPS服务。<br>如果您在网站A的接入配置中自定义了HTTP 80、8080端口，那么在网站B的接入配置中，您最多可以自定义8个不同的HTTPS端口。 |

| 参数 | 适用的实例类型 | 说明 |
| --- | --- | --- |
| Cname Reuse | DDoS高防（国际） | 选择是否开启CNAME复用。<br>该功能适用于同一台服务器上有多个网站业务的场景。开启CNAME复用后，您只需将同一个服务器上多个域名的解析指向同一个高防CNAME地址，即可将多个域名接入高防，无需为每个域名分别添加高防网站配置。更多信息，请参见CNAME复用。 |

ii. **完成配置。**


按照页面提示，完成以下后续步骤：

a. 放行DDoS高防回源IP：

如果源站服务器上安装了防火墙等安全软件，您需要在源站放行DDoS高防回源IP，避免由高防转发回源站的流量被误拦截。

如果不存在上述情况，请跳过该步骤。

b. 更换源站ECS公网IP：

如果您的源站是阿里云ECS服务器，且源站IP地址不慎暴露，您需要更换ECS云服务器的公网IP，防止黑客绕过DDoS高防直接攻击源站。

如果不存在上述情况，请跳过该步骤。

c. 上传HTTPS证书：

如果接入高防的网站有HTTPS业务，您必须将域名关联的HTTPS证书上传到DDoS高防实例中配置的对应域名，才能保证HTTPS协议请求被正常响应。

> **说明** 如果网站已关联增强型DDoS高防实例，则在成功上传HTTPS证书后，您还可以为网站自定义TLS安全策略。具体操作，请参见自定义TLS安全策略。

如果网站只有HTTP业务，请跳过该步骤。

d. （可选）本地验证转发配置生效：

在本地计算机上验证添加到高防的网站配置已经生效，避免在网站配置未生效时将业务流量切换到高防，导致业务中断。

e. 修改域名的解析设置：

添加网站配置后，DDoS高防为网站分配一个CNAME地址，您必须将网站域名的DNS解析指向高防CNAME地址，才可以正式将业务流量切换到高防实例进行防护。您可以手动修改网站域名的DNS解析或者使用NS接入的方式自动修改DNS解析。

相关操作，请参见手动修改DNS解析接入网站业务、NS方式接入网站业务。

iii. 单击**去网站列表**，您可以在网站列表中查看新添加的网站域名和域名对应的高防CNAME地址。

完成**添加网站**配置向导后，您可以对已经添加的网站配置执行以下操作：


- 添加备注：单击**备注**后的

  图标，为该网站配置添加备注信息，便于后续识别。
- **编辑**、**删除**：编辑、删除已添加的网站配置。

> **注意** 您可以通过编辑网站配置，开启高防流量标记功能，使DDoS高防在回源请求的自定义Header字段记录特定的信息。该功能可用于获取客户端真实源端口、记录高防转发流量等场景。更多信息，请参见设置流量标记。

- **DNS设置**：如果您开启了付费版的阿里云云解析DNS服务，则可以使用NS接入方式自动修改域名DNS，完成业务流量切换到高防进行防护。

  具体操作，请参见NS方式接入网站业务。
- **防护设置**：前往**网站业务DDoS防护**页签，修改网站的DDoS防护功能配置。

  成功添加网站配置后，DDoS高防默认为网站开启**AI智能防护**和**频率控制**防护功能，您可以在**网站业务DDoS防护**页签，为网站开启更多的防护功能和修改防护功能的规则。

  具体操作，请参见设置AI智能防护。
- **回源设置**：如果接入高防的网站有多个源站服务器，您可以通过回源设置修改**回源负载算法**。

  具体操作，请参见修改回源设置。

## 后续配置

完成域名接入流程后，网站访问流量将经过DDoS高防保护，您还需要完善以下配置，才能更好地防护网站安全。

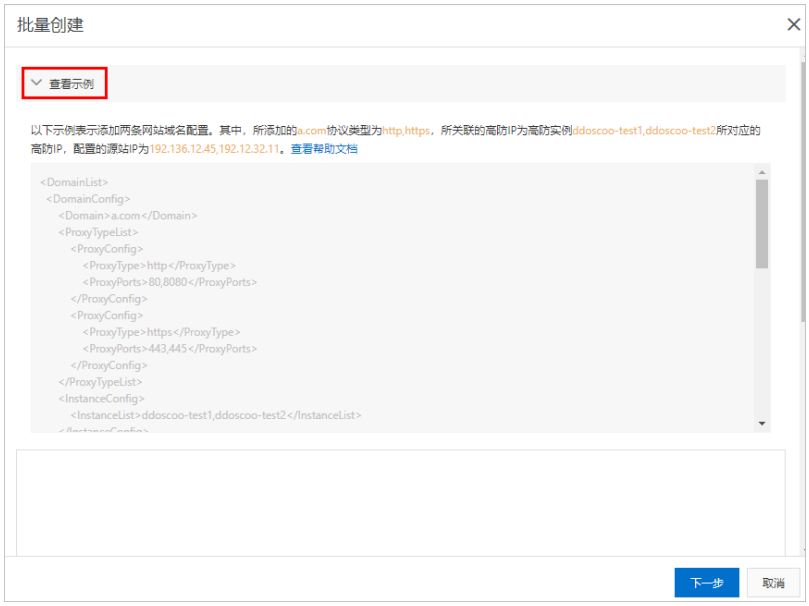
| 配置类型 | 说明 | 相关文档 |
| --- | --- | --- |
| 网站业务DDoS防护配置 | DDoS高防默认为接入防护的网站开启了**全局防护策略**、**AI智能防护**和**频率控制**防护功能，您可以在**网站业务DDoS防护**页签，为网站开启更多的防护功能、修改防护功能的规则。 | • 设置DDoS全局防护策略<br>• 设置AI智能防护<br>• 设置黑白名单（针对域名）<br>• 设置区域封禁（针对域名）<br>• 设置精准访问控制<br>• 设置频率控制 |
| 云监控告警配置 | 通过配置云监控告警规则，您可以针对DDoS高防的常用业务指标（例如，高防IP流量、连接数等）、攻击事件（例如，黑洞、清洗事件）设置告警规则，使云监控在高防上业务发生异常时，及时向您发送告警，帮助您缩短响应时间，尽快恢复业务。 | 设置云监控告警 |
| 全量日志服务配置 | 通过启用全量日志服务，您可以使DDoS高防采集并存储网站业务的全量日志数据，供您进行业务查询与分析。DDoS高防全量日志服务默认存储180天内的网站全量日志，帮助您满足等保合规要求。 | 快速上手 |

## 批量导入网站配置

1. 登录DDoS高防控制台。
2. 在顶部菜单栏左上角处，选择服务所在地域：
   - **中国内地**：选择该地域将跳转到**DDoS高防（新BGP）**控制台。
   - **非中国内地**：选择该地域将跳转到**DDoS高防（国际）**控制台。

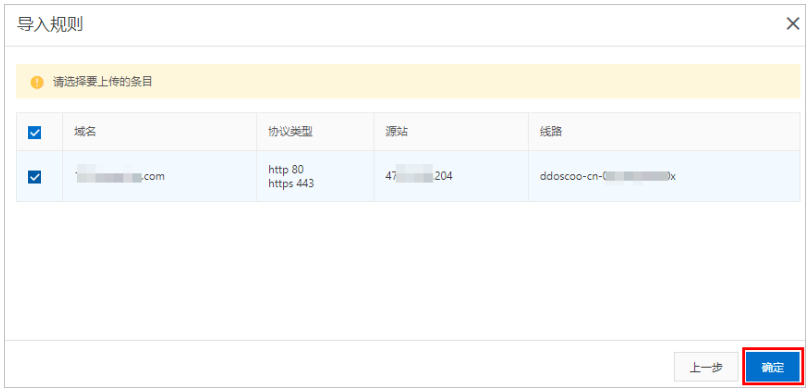
     您可以通过切换地域分别管理和配置DDoS高防（新BGP）和DDoS高防（国际）实例。在使用DDoS高防服务时，请确认您已选择正确的地域。
3. 在左侧导航栏，选择**接入管理 > 域名接入**。
4. 在**域名接入**页面，单击网站列表下方的**批量导入**。
5. 在**批量创建**面板，输入要导入的网站配置，并单击**下一步**。

   批量创建的网站配置采用XML文件格式传入。关于文件格式的说明，请参见网站配置XML格式说明。




如果您填写的XML配置参数文本内容正确，则XML配置将被解析成所需导入的网站配置。

6. 在**导入规则**面板，选中要导入的网站配置，并单击**确定**。




7. 成功上传网站配置后，关闭**上传完成**面板。

# 4.1.2. 本地验证转发配置生效

成功添加DDoS高防网站或端口配置后，DDoS高防预期会把请求高防IP对应端口的报文转发到源站（真实服务器）的对应端口。为了保证业务的稳定，我们建议您在进行业务接入高防配置前先完成本地验证，确保转发配置已经生效。本文将指导您完成本地验证。

## 前提条件

- 已在DDoS高防控制台添加网站或端口配置。更多信息，请参见添加网站、添加规则。
- 已在源站服务器上设置放行DDoS高防回源IP。更多信息，请参见放行DDoS高防回源IP。

## 背景信息

对于需要通过域名访问的业务（例如客户端中使用的服务器地址是域名而不是IP），在为该类型业务接入DDoS高防时，您需要添加网站配置。添加网站配置后，您可以通过修改本地hosts文件或者使用高防CNAME地址访问服务器的方式验证转发配置生效。

有的四层业务（例如游戏业务）可能不需要域名，直接通过IP进行交互。在为该类型业务接入DDoS高防时，您需要添加端口转发规则。添加转发规则后，您可以通过使用高防IP访问服务器的方式验证转发配置生效。

> **注意** 如果转发配置未生效就执行业务切换，将可能导致业务中断。

## 修改本地hosts文件

1. 修改本地hosts文件，使本地对于被防护站点的请求经过高防。以Windows操作系统为例，操作步骤如下。
   i. 定位到hosts文件。一般hosts文件存储在*C:\Windows\System32\drivers\etc*\文件夹下。
   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`。

   例如高防IP是`180.xx.xx.173`，域名是`www.aliyundemo.com`，则在hosts文件最后一行添加的内容为`180.xx.xx.173 www.aliyundemo.com`。

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

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

   iv. 保存修改后的hosts文件。
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，请尝试刷新本地的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。

## 使用高防CNAME地址访问服务器

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

> **说明** 成功添加网站配置后，DDoS高防为域名分配一个CNAME地址，用于业务接入配置。您可以在域名接入配置列表中查看域名对应的CNAME地址。

如果无法正常访问，请确认前提条件中的配置正确。如问题依然存在，请联系阿里云售后技术支持。

## 使用高防IP访问服务器

假设高防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。

添加端口配置后，您可以直接在本地通过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。

如果本地客户端支持直接填写服务器IP，您也可以直接填入高防IP进行测试。

# 4.1.3. 修改网站业务的回源设置

您可以通过回源设置，为已添加到DDoS高防防护的网站业务设置回源负载均衡算法。

## 前提条件

已添加网站业务到DDoS高防进行防护。相关操作，请参见添加网站。

## 背景信息

如果您在添加网站时设置了多个服务器地址（多个源站IP或多个源站域名），则DDoS高防实例在转发网站业务流量到源站服务器时，默认采用轮询算法实现服务器负载均衡。您可以修改回源负载均衡算法或者为不同服务器设置权重。

支持的负载均衡算法如下表所示。

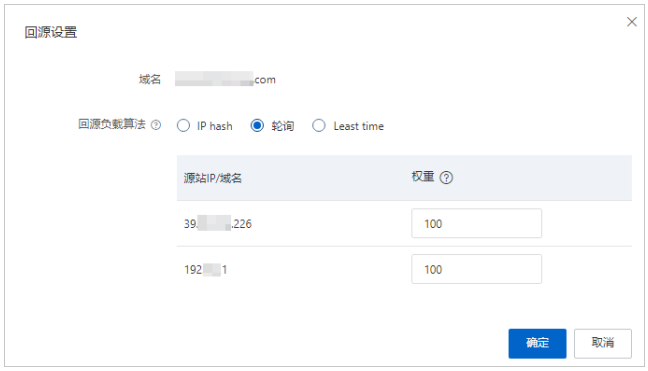
| 算法名称 | 说明 |
| --- | --- |
| **IP hash** | 将某个IP的请求固定转发到一个服务器地址。 |
| **轮询**（默认） | 所有请求轮流分配给所有服务器地址。默认所有服务器地址具有相同权重。<br>支持修改服务器权重。服务器权重越大，被分配到请求的可能性越高。 |
| **Least time** | 通过智能DNS解析能力和Least time回源算法，保证业务流量将从接入防护节点到转发回源站服务器整个链路的时延最短。 |

## 操作步骤

1. 登录DDoS高防控制台。
2. 在顶部菜单栏左上角处，选择服务所在地域：
   - **中国内地**：选择该地域将跳转到**DDoS高防（新BGP）**控制台。
   - **非中国内地**：选择该地域将跳转到**DDoS高防（国际）**控制台。

     您可以通过切换地域分别管理和配置DDoS高防（新BGP）和DDoS高防（国际）实例。在使用DDoS高防服务时，请确认您已选择正确的地域。
3. 在左侧导航栏，选择**接入管理 > 域名接入**。
4. 定位到要设置的域名，单击**操作**列下的**回源设置**。
5. 在**回源设置**对话框，选择**回源负载算法**。

   支持的算法包括：**IP hash**、**轮询**、**Least time**。关于不同算法的说明，请参见算法说明。




6. 如果在上一步选择了**轮询**算法，您还可以为不同源站地址设置**权重**；如果选择了其他算法，请跳过该步骤。

   权重使用1~100范围内的整数表示。权重越大，源站地址被分配到回源请求的可能性越高。
7. 单击**确定**。

   回源设置成功后，DDoS高防实例将按照您设置的回源负载均衡算法实现多服务器间负载均衡。

# 4.1.4. 编辑网站

您可以通过编辑已创建的网站配置，为网站重新关联DDoS高防实例（例如由标准功能套餐更换为增强功能套餐）、修改源站IP等。编辑网站配置支持批量操作。本文介绍了编辑网站配置和批量修改网站配置的具体操作。

## 前提条件

已在DDoS高防（新BGP）、DDoS高防（国际）下创建网站配置。相关操作，请参见添加网站。

## 编辑网站配置

1. 登录DDoS高防控制台。
2. 在顶部菜单栏左上角处，选择服务所在地域：
   - **中国内地**：选择该地域将跳转到**DDoS高防（新BGP）**控制台。
   - **非中国内地**：选择该地域将跳转到**DDoS高防（国际）**控制台。

     您可以通过切换地域分别管理和配置DDoS高防（新BGP）和DDoS高防（国际）实例。在使用DDoS高防服务时，请确认您已选择正确的地域。
3. 在左侧导航栏，选择**接入管理 > 域名接入**。
4. 定位到要编辑的网站配置，单击其操作列下的**编辑**。

   > **说明** 您也可以批量修改网站配置。具体操作，请参见批量修改网站配置。

5. 在**编辑网站**页面，修改网站配置信息，并单击**确定**。

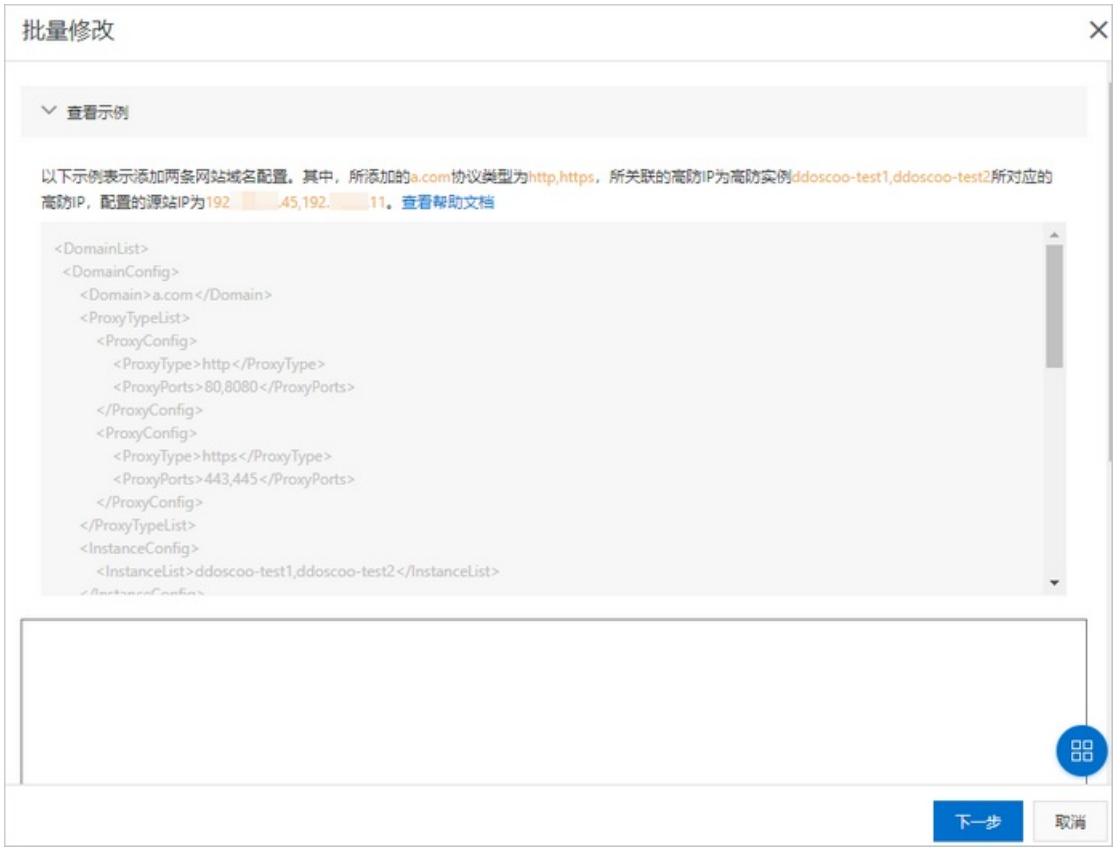
   您可以修改除网站域名以外的配置信息。例如，重新选择**功能套餐**和**实例**，为网站关联其他DDoS高防实例；或者重新输入**源站IP**，更新源站IP等。关于网站配置的描述，请参见网站配置说明。

## 批量修改网站配置

1. 登录DDoS高防控制台。
2. 在顶部菜单栏左上角处，选择服务所在地域：
   - **中国内地**：选择该地域将跳转到**DDoS高防（新BGP）**控制台。
   - **非中国内地**：选择该地域将跳转到**DDoS高防（国际）**控制台。

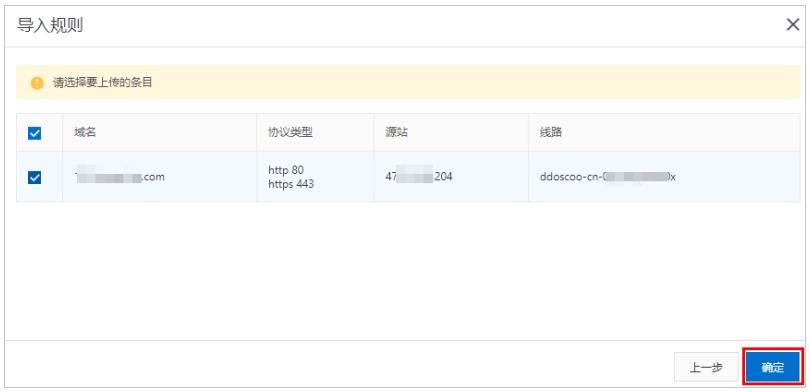
     您可以通过切换地域分别管理和配置DDoS高防（新BGP）和DDoS高防（国际）实例。在使用DDoS高防服务时，请确认您已选择正确的地域。
3. 在左侧导航栏，选择**接入管理 > 域名接入**。
4. 在**域名接入**页面，单击网站列表下方的**批量修改**。
5. 在**批量修改**页面，输入新的网站配置，并单击**下一步**。

   批量修改的网站配置采用XML文件格式传入，关于文件格式的说明，请参见网站配置XML格式说明。




如果输入的XML配置参数文本内容正确，则其将被解析成所需导入的网站配置。

6. 在**导入规则**面板，选中要导入的网站配置，并单击**确定**。




7. 成功上传网站配置后，关闭**上传完成**面板。

# 4.1.5. 删除网站

若您的网站不再需要接入DDoS高防，您必须先为其恢复域名解析，即确保域名的DNS解析中不再使用高防IP、高防CNAME、流量调度器CNAME作为记录值，然后删除对应的网站配置。若您未恢复网站域名解析就删除网站配置，则可能导致业务中断。

## 前提条件

已恢复网站域名解析。

## 操作步骤

1. 登录DDoS高防控制台。
2. 在顶部菜单栏左上角处，选择服务所在地域：
   - **中国内地**：选择该地域将跳转到**DDoS高防（新BGP）**控制台。
   - **非中国内地**：选择该地域将跳转到**DDoS高防（国际）**控制台。

     您可以通过切换地域分别管理和配置DDoS高防（新BGP）和DDoS高防（国际）实例。在使用DDoS高防服务时，请确认您已选择正确的地域。
3. 在左侧导航栏，选择**接入管理 > 域名接入**。
4. 定位到要删除的网站配置，单击其操作列下的**删除**。

   > **说明** 如果您使用DDoS高防（新BGP）服务，则您也可以批量删除多个网站配置。您可以勾选要删除的网站配置，单击网站列表下方的**批量删除**。
5. 在删除提示对话框中，确认删除操作。

# 4.1.6. 批量导出

DDoS高防网站配置支持批量导出。您可以将DDoS高防的全部网站配置以XML格式导出并下载到本地。批量导出的网站配置格式与批量导入/修改网站配置保持一致。

## 操作步骤

1. 登录DDoS高防控制台。
2. 在顶部菜单栏左上角处，选择服务所在地域：
   - **中国内地**：选择该地域将跳转到**DDoS高防（新BGP）**控制台。
   - **非中国内地**：选择该地域将跳转到**DDoS高防（国际）**控制台。

     您可以通过切换地域分别管理和配置DDoS高防（新BGP）和DDoS高防（国际）实例。在使用DDoS高防服务时，请确认您已选择正确的地域。
3. 在左侧导航栏，选择**接入管理 > 域名接入**。
4. 在网站列表下方，单击**批量导出**，下发导出任务。
5. 导出任务已下发后，单击页面右上角的任务图标。


6. 在**任务列表**侧边页，等待任务打包完成后，单击**下载**，下载导出文件到本地。

   > **说明** 如果当前任务状态为**待执行**状态，请耐心等待导出任务完成。


成功下载导出文件到本地后，您可以使用文本编辑工具打开下载的*.xml*文件，查看网站配置内容。更多信息，请参见网站配置XML格式说明。

> **说明** 如果您使用DDoS高防（新BGP）服务，则导出文件的名称以*DDoSCoo_*开头。如果您使用DDoS高防（国际）服务，则导出文件的名称以*DDoSDip_*开头。使用DDoS高防（新BGP）和DDoS高防（国际）服务导出的内容格式相同。

```
<?xml version="1.0" encoding="UTF-8"?><DomainList>
<DomainConfig>
<Domain>[redacted]com</Domain>
<ProxyTypeList>
<ProxyConfig>
<ProxyType>websockets</ProxyType>
<ProxyPorts>443</ProxyPorts>
</ProxyConfig>
<ProxyConfig>
<ProxyType>http</ProxyType>
<ProxyPorts>80,3333,3501</ProxyPorts>
</ProxyConfig>
<ProxyConfig>
<ProxyType>https</ProxyType>
<ProxyPorts>443</ProxyPorts>
</ProxyConfig>
<ProxyConfig>
<ProxyType>websocket</ProxyType>
<ProxyPorts>80,3333,3501</ProxyPorts>
</ProxyConfig>
</ProxyTypeList>
<InstanceConfig>
<InstanceList>ddoscoo-cn-[redacted]ddoscoo-cn-[redacted]</InstanceList>
</InstanceConfig>
<RealServerConfig>
<ServerType>0</ServerType>
<ServerList>47.[redacted]204</ServerList>
</RealServerConfig>
</DomainConfig>
</DomainList>
```

7. （可选）在**任务列表**侧边页，定位到不再需要的任务，单击**删除**，将其移除。

# 4.1.7. 自定义服务器端口

DDoS高防默认防护通过80端口（HTTP）、443端口（HTTPS）提供服务的网站业务。如果您的网站业务使用80、443以外的端口提供服务，则在接入网站业务到DDoS高防实例防护时，您需要在网站配置中自定义服务器端口。

## 自定义端口的限制

自定义服务器端口有以下要求：

- 自定义端口必须在DDoS高防提供的端口范围内。DDoS高防实例的**功能套餐**不同，支持的可选端口范围不同，具体说明如下：
  - **标准功能**实例：
    - HTTP协议可选端口：80、8080。

    - HTTPS协议可选端口：443、8443。
  - **增强功能**实例：
    - HTTP协议可选端口范围：80~65535。
    - HTTPS协议可选端口范围：80~65535。
- 所有接入DDoS高防实例防护的网站业务下自定义的不同端口（包含不同协议下的自定义端口）的总数不能超过10个。

  示例：假设您有2个网站（A和B）要接入DDoS高防实例防护，网站A提供HTTP服务、网站B提供HTTPS服务。

  如果您在网站A的接入配置中自定义了HTTP 80、8080端口，那么在网站B的接入配置中，您最多可以自定义8个不同的HTTPS端口。

## 操作步骤

以下操作步骤以修改已添加的网站配置为例，介绍自定义服务器端口的方法。您也可以在添加网站时自定义服务器端口，具体操作，请参见添加网站。

1. 登录DDoS高防控制台。
2. 在顶部菜单栏左上角处，选择服务所在地域：
   - **中国内地**：选择该地域将跳转到**DDoS高防（新BGP）**控制台。
   - **非中国内地**：选择该地域将跳转到**DDoS高防（国际）**控制台。

     您可以通过切换地域分别管理和配置DDoS高防（新BGP）和DDoS高防（国际）实例。在使用DDoS高防服务时，请确认您已选择正确的地域。
3. 在左侧导航栏，选择**接入管理 > 域名接入**。
4. 定位到要编辑的网站配置，单击**操作**列下的**编辑**。
5. 在网站配置页面，定位到**服务器端口**配置项，单击**自定义**。

   
   
6. 分别选中**HTTP**、**HTTPS**协议，在输入框中填写提供对应服务的自定义端口，并单击**保存**。

   多个端口间使用半角逗号（,）分隔。您可以单击**查看可选范围**，查看HTTP或HTTPS协议支持的可选端口范围。

   
   
7. 单击**确定**，并在**确定**对话框确认已修改的内容。

# 4.1.8. 上传HTTPS证书

要使DDoS高防帮助您清洗HTTPS业务流量，您必须在网站配置中选择HTTPS协议并上传HTTPS证书。已上传证书发生变化时，您也要在DDoS高防控制台及时更新证书。

## 前提条件

- 已添加网站配置且网站支持HTTPS协议。更多信息，请参见添加网站。
- 已准备好证书文件内容。

  如果您已将证书文件上传到SSL证书服务控制台进行统一管理，那么在上传证书时您可以直接选择已有证书，否则您需要准备好网站的证书和私钥文件。您需要准备的证书相关内容包括：

  - 公钥文件（CRT格式）或者证书文件（PEM格式）
  - 私钥文件（KEY格式）

## 应用场景

您需要在以下场景中上传HTTPS证书：

- 接入域名时，域名的协议是HTTPS协议。
- 接入HTTPS协议的域名后，已上传的证书需要更换或因为证书过期需要更新。

## 操作步骤

1. 登录DDoS高防控制台。
2. 在顶部菜单栏左上角处，选择服务所在地域：
   - **中国内地**：选择该地域将跳转到**DDoS高防（新BGP）**控制台。
   - **非中国内地**：选择该地域将跳转到**DDoS高防（国际）**控制台。

     您可以通过切换地域分别管理和配置DDoS高防（新BGP）和DDoS高防（国际）实例。在使用DDoS高防服务时，请确认您已选择正确的地域。
3. 在左侧导航栏，选择**接入管理 > 域名接入**。
4. 在**域名接入**页面，定位到要操作的域名，单击**证书状态**列下的上传图标。


5. 在**上传证书和私钥**对话框，选择一种**上传方式**，并完成上传配置。

   可选择的上传方式包括：

   - **（推荐）选择已有证书**

     如果您的网站证书已经上传并托管在SSL证书服务中，您可以直接从已有证书中选择证书并上传。


     即使您的证书未托管在SSL证书服务，您也可以单击**前往SSL证书控制台管理**，上传并管理您的证书，然后再选择已有证书。关于如何在SSL证书服务控制台上传证书，请参见上传证书。

- **手动上传**

  填写**证书名称**，并将证书文件和私钥文件中的文本内容分别复制粘贴到**证书文件**和**私钥文件**框中。


> **说明**
>
> - 对于PEM、CER、CRT格式的证书，您可以使用文本编辑器直接打开证书文件，复制其中的文本内容。对于其他格式（例如，PFX、P7B等）的证书，您需要将证书文件转换成PEM格式后，才能用文本编辑器打开并复制其中的文本内容。关于证书格式的转换方式，请参见HTTPS证书转换成PEM格式。
> - 如果该HTTPS证书有多个证书文件（例如，证书链），您需要将证书文件中的文本内容拼接合并后粘贴至**证书文件**中。

证书文件文本内容样例：

```
-----BEGIN CERTIFICATE-----
xxxxxxxxxxxxvs6MTXcJSfN9Z7rZ9fmxWr2BFN2XbahgnsSXM48ixZJ4krc+1M+j2kcubVpsE2cgHdj4v8H6j
Uz9Ji4mr7vMNS6dXv8PUkl/qoDeNGCNdyTS5NIL5ir+g92cL8IGOkjgvhlqt9vc65Cgb4mL+n5+DV9uOyTZTW
/MojmlgfUekC2xiXa54nxJf17Y1TADGSbyJbsC0Q9nIrHsPl8YKkvRWvIAqYxXZ7wRwWWmv4TMxFhWRiNY7yZ
Io2ZUhl02SIDNggIEeg==
-----END CERTIFICATE-----
```

私钥文件文本内容样例：

```
-----BEGIN RSA PRIVATE KEY-----
xxxxxxxxxxxxtZ3UKHJTRgNQmioPQn2bqdKHop+B/dn/4VZL7Jt8zSDGM9sTMThLyvsmLQKBgQCr+ujntC1kN
6pGBj2Fw2l/EA/W3rYEce2tyhjgmG7rZ+A/jVE9fld5sQra6ZdwBcQJaiygoIYoaMF2EjRwc0qwHaluq0C15f
6ujSoHh2e+D5zdmkTg/3NKNjqNv6xA2gYpinVDzFdZ9Zujxvuh9o4Vqf0YF8bv5UK5G04RtKadOw==
-----END RSA PRIVATE KEY-----
```

6. 单击**确定**。
   成功上传证书后，**证书状态**会变更为**正常**。


如果证书发生更新，您必须及时在DDoS高防控制台的**域名接入**页面修改证书（单击证书后的图标），上传更新后的证书。

> 警告　如果证书已经更新，却没有在DDoS高防控制台修改证书，将会导致HTTPS业务解析异常。

## 相关FAQ

证书与密钥不匹配问题排查

# 4.1.9. 自定义TLS安全策略

DDoS高防支持TLS安全策略自定义功能，您可以根据实际业务需要，为已接入DDoS高防防护的网站业务设置合适的TLS协议版本和加密算法套件。本文介绍了修改TLS安全策略的具体操作。

## 前提条件

- 已添加网站配置，且网站配置关联了**增强功能**套餐的DDoS高防实例。相关操作，请参见添加网站。

  目前仅增强功能套餐的DDoS高防实例支持自定义TLS配置。如果您使用标准功能套餐的DDoS高防实例，建议您升级DDoS高防实例到增强功能套餐后，再使用该功能。关于升级DDoS高防实例的具体操作，请参见升级实例。
- 网站配置的**协议类型**包含**HTTPS**，且已上传对应的HTTPS证书。相关操作，请参见上传HTTPS证书。

## 背景信息

DDoS高防实例支持设置的TLS协议版本包含1.0/1.1/1.2/1.3。接入DDoS高防（新BGP）实例防护的网站业务默认支持TLS 1.0、1.1和1.2版本，接入DDoS高防（国际）实例防护的网站业务默认支持TLS 1.1和1.2版本。如果上述默认配置不能满足您的业务需求，您可以手动修改TLS安全策略。

例如，假设您的业务需要通过PCI DSS 3.2认证，希望禁用TLS 1.0协议，而您的另一个业务的访问终端仅支持TLS 1.0协议，需要兼容TLS 1.0协议。这种情况下，您可以通过TLS安全策略自定义功能为不同业务灵活配置所需的TLS安全策略。

## 操作步骤

1. 登录DDoS高防控制台。
2. 在顶部菜单栏左上角处，选择服务所在地域：
   - **中国内地**：选择该地域将跳转到**DDoS高防（新BGP）**控制台。
   - **非中国内地**：选择该地域将跳转到**DDoS高防（国际）**控制台。

     您可以通过切换地域分别管理和配置DDoS高防（新BGP）和DDoS高防（国际）实例。在使用DDoS高防服务时，请确认您已选择正确的地域。
3. 在左侧导航栏，选择**接入管理 > 域名接入**。
4. 定位到要操作的域名，单击**证书状态**列中的**TLS安全策略**。

> **注意** 只有当域名关联了**增强功能**套餐的DDoS高防实例，且**协议类型**包含**HTTPS**、**证书状态**为**正常**时，才支持设置TLS安全策略。


5. 在**TLS安全策略配置**对话框，配置**TLS版本**和**加密套件**。


| 参数 | 说明 |
| --- | --- |
| **TLS版本** | 选择HTTPS支持的TLS协议版本。可选项：<br>○ **支持TLS1.0及以上版本，兼容性最好，安全性较低**（默认）：支持TLS 1.0、TLS 1.1和TLS 1.2。<br>○ **支持TLS1.1及以上版本，兼容性较好，安全性较好**：支持TLS 1.1和TLS 1.2。<br>○ **支持TLS1.2及以上版本，兼容性较好，安全性很高**：支持TLS 1.2。<br>您也可以根据需要选择**开启支持TLS1.3**。 |
| | 选择HTTPS支持的加密套件。可选项：<br>**说明** 您可以将光标放置在某个加密套件选项上的 图标，查看该选项包含的加密套件。<br>○ **全部加密套件，安全性较低，兼容性较高**（默认）<br>该选项包含以下加密套件：<br>■ ECDHE-ECDSA-AES128-GCM-SHA256<br>■ ECDHE-ECDSA-AES256-GCM-SHA384<br>■ ECDHE-ECDSA-AES128-SHA256<br>■ ECDHE-ECDSA-AES256-SHA384<br>■ ECDHE-RSA-AES128-GCM-SHA256<br>■ ECDHE-RSA-AES256-GCM-SHA384<br>■ ECDHE-RSA-AES128-SHA256 |

| 参数 | 说明 |
| --- | --- |
| 加密套件 | ■ ECDHE-RSA-AES256-SHA384<br>■ AES128-GCM-SHA256<br>■ AES256-GCM-SHA384<br>■ AES128-SHA256 AES256-SHA256<br>■ ECDHE-ECDSA-AES128-SHA<br>■ ECDHE-ECDSA-AES256-SHA<br>■ ECDHE-RSA-AES128-SHA<br>■ ECDHE-RSA-AES256-SHA<br>■ AES128-SHA AES256-SHA<br>■ DES-CBC3-SHA<br>○ **强加密套件，安全性较高，兼容性较低**：只有在TLS版本为支持TLS1.2及以上版本，兼容性较好，安全性很高时，支持该选项。<br>该选项包含以下加密套件：<br>■ ECDHE-ECDSA-AES128-GCM-SHA256<br>■ ECDHE-ECDSA-AES256-GCM-SHA384<br>■ ECDHE-ECDSA-AES128-SHA256<br>■ ECDHE-ECDSA-AES256-SHA384<br>■ ECDHE-RSA-AES128-GCM-SHA256<br>■ ECDHE-RSA-AES256-GCM-SHA384<br>■ ECDHE-RSA-AES128-SHA256<br>■ ECDHE-RSA-AES256-SHA384<br>■ ECDHE-ECDSA-AES128-SHA<br>■ ECDHE-ECDSA-AES256-SHA<br>○ **自定义加密套件**：选择该选项后，您需要从全部加密套件中选择一个或多个加密套件。 |

6. 单击**确定**。

## 执行结果

为网站业务修改TLS安全策略后，DDoS高防实例在处理网站域名的请求流量时，会采用已配置的TLS协议版本及加密套件。如果客户端请求使用了不支持的TLS协议版本，则该请求将被丢弃。

# 4.1.10. 设置流量标记

网站业务接入DDoS高防后，您可以通过设置高防流量标记，开启获取客户端真实端口功能，以及使高防转发到源站的流量中包含特定的自定义Header字段值，方便您的后端服务器对高防转发的流量进行统计分析。本文介绍了设置高防流量标记的具体操作。

## 前提条件

已添加网站配置。更多信息，请参见添加网站。

## 操作步骤

1. 登录DDoS高防控制台。
2. 在顶部菜单栏左上角处，选择服务所在地域：
   - **中国内地**：选择该地域将跳转到**DDoS高防（新BGP）**控制台。
   - **非中国内地**：选择该地域将跳转到**DDoS高防（国际）**控制台。

     您可以通过切换地域分别管理和配置DDoS高防（新BGP）和DDoS高防（国际）实例。在使用DDoS高防服务时，请确认您已选择正确的地域。
3. 在左侧导航栏，选择**接入管理 > 域名接入**。
4. 定位到要操作的网站配置，单击**操作**列下的**编辑**。
5. 在网站配置编辑页面，定位到**流量标记**区域，完成以下配置。


| 参数 | 说明 |
| --- | --- |
| **获取客户端真实端口** | 如果您需要获取请求客户端使用的真实端口，则可以打开该开关。<br>打开该开关后，高防在代理网站流量时，默认使用 `X-Forwarded-ClientSrcPort` 字段记录真实的客户端源端口。您可以从高防转发到源站的请求中解析 `X-Forwarded-ClientSrcPort` 字段，获取客户端使用的真实端口。具体操作与获取客户端真实请求IP类似，更多信息，请参见配置DDoS高防后获取真实的请求来源IP。 |
| **其他自定义Header** | 您可以在此处添加自定义的Header字段（包含字段名称和字段值）。<br>添加自定义Header字段后，高防在代理网站流量时，会在转发到源站的请求中添加对应的字段值，方便您后端的服务进行统计分析。<br>添加自定义Header注意事项：<br>○ 请不要使用以下默认字段作为自定义Header：<br>■ `X-Forwarded-ClientSrcPort`：默认被用于获取访问高防七层引擎的客户端端口。<br>■ `X-Forwarded-ProxyPort`：默认被用于获取访问高防七层引擎的监听端口。<br>○ 请不要使用标准HTTP头部字段（例如，user-agent等），否则会导致请求原始头部字段的内容被改写。<br>○ 最多支持添加5个自定义Header。 |

6. 单击**确定**。

## 相关操作

配置DDoS高防后获取真实的请求来源IP

# 4.1.11. 网站配置XML格式说明

批量操作DDoS高防网站配置时（例如批量导入、修改、导出），网站配置按照固定的XML格式传递。本文介绍了网站配置的XML格式。

## 参数说明

网站配置参数内容必须以 `<DomainList>` 开始， `</DomainList>` 结束，中间部分是网站配置的参数信息。其中，每个网站的配置参数均以 `<DomainConfig>` 开始， `</DomainConfig>` 结束，中间部分为与该网站配置相关的具体参数，详见下表。

> **说明** 每多添加一个网站配置，则增加一个 `<DomainConfig>……</DomainConfig>` 数据结构体。

| 网站配置具体参数 | 说明 |
| --- | --- |
| `<Domain>a.aliyundoc.com</Domain>` | 待配置的域名。只能设置一个域名。 |
| `<ProtocolConfig> <ProtocolList>http,https</ProtocolList> </ProtocolConfig>` | 域名协议类型。多个协议类型间以半角逗号（,）隔开。本示例表示该域名的协议类型为HTTP和HTTPS。 |
| `<InstanceConfig> <InstanceList>ddoscoo-cn-zvp2eibz**** </InstanceList> </InstanceConfig>` | 网站关联的DDoS高防实例。<br>> **说明** 由于每个DDoS高防实例对应一个ID，所以只需填写DDoS高防实例ID即可。多个实例ID间以半角逗号（,）隔开。 |
| `<RealServerConfig> <ServerType>0</ServerType> <ServerList>192.0.XX.XX</ServerList> </RealServerConfig>` | 源站信息。结构说明如下：<br>• `<ServerType>0</ServerType>` ：表示源站IP。<br>• `<ServerType>1</ServerType>` ：表示源站域名。<br>`<ServerList>192.0.XX.XX</ServerList>` 表示源站地址，多个地址间以半角逗号（,）隔开。<br>> **说明** 配置某个域名的源站信息时，只能是源站IP或源站域名信息，两者不能同时存在。 |

## 示例

```
<DomainList>
 <DomainConfig>
 <Domain>a.aliyundoc.com</Domain>
 <ProtocolConfig>
 <ProtocolList>http,https</ProtocolList>
 </ProtocolConfig>
 <InstanceConfig>
 <InstanceList>ddoscoo-cn-zvp2eibz****</InstanceList>
 </InstanceConfig>
 <RealServerConfig>
 <ServerType>0</ServerType>
 <ServerList>192.0.XX.XX</ServerList>
 </RealServerConfig>
 </DomainConfig>
 <DomainConfig>
 <Domain>b.aliyundoc.com</Domain>
 <ProtocolConfig>
 <ProtocolList>http,websocket,websockets</ProtocolList>
 </ProtocolConfig>
 <InstanceConfig>
 <InstanceList>ddoscoo-cn-7pp2e74f****, ddoscoo-cn-2r42e12c****</InstanceList>
 </InstanceConfig>
 <RealServerConfig>
 <ServerType>1</ServerType>
 <ServerList>q840a82zf2j23afs.aliyundoc.com</ServerList>
 </RealServerConfig>
 </DomainConfig>
 </DomainList>
```

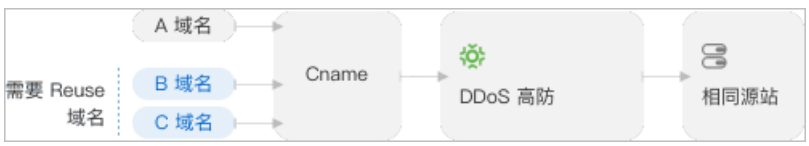
该示例表示添加以下两条网站配置：

- 网站一：域名是a.aliyundoc.com，协议类型是HTTP和HTTPS，关联高防实例ddoscoo-cn-zvp2eibz****，对应源站IP是192.0.XX.XX。
- 网站二：域名b.aliyundoc.com，协议类型是HTTP、WebSocket和WebSockets，关联高防实例ddoscoo-cn-7pp2e74f****和 ddoscoo-cn-2r42e12c****，对应源站域名q840a82zf2j23afs.aliyundoc.com。

# 4.1.12. CNAME复用

如果您在一个服务器上有多个网站域名需要接入DDoS高防（国际），您可以申请开通CNAME复用，实现只添加一次高防配置，而使高防配置的CNAME地址供多个域名复用。

开启CNAME复用后，您只需将同服务器上多个域名的解析指向高防CNAME地址，即可将多个域名接入高防，无需为每个域名分别添加高防配置。




## 前提条件

已提交工单申请开放CNAME复用功能。本文操作描述建立在已开放CNAME复用的前提下。

> **说明** 仅DDoS高防（国际）服务支持CNAME复用。如果您使用DDoS高防（新BGP）服务，则暂时不支持使用CNAME复用。

## 使用场景

CNAME复用适用于以下场景，以避免对多个域名重复添加高防配置：

- 场景1：代理商、ISV、分销商有大量域名（大部分域名的源站是同一个服务器）需要接入DDoS高防，且域名有频繁增删的情况。
- 场景2：同一个业务使用大量不同一级域名做推广、SEO。
- 场景3：同一个业务使用大量备用域名。

## 使用限制

下表描述了CNAME复用的使用限制。

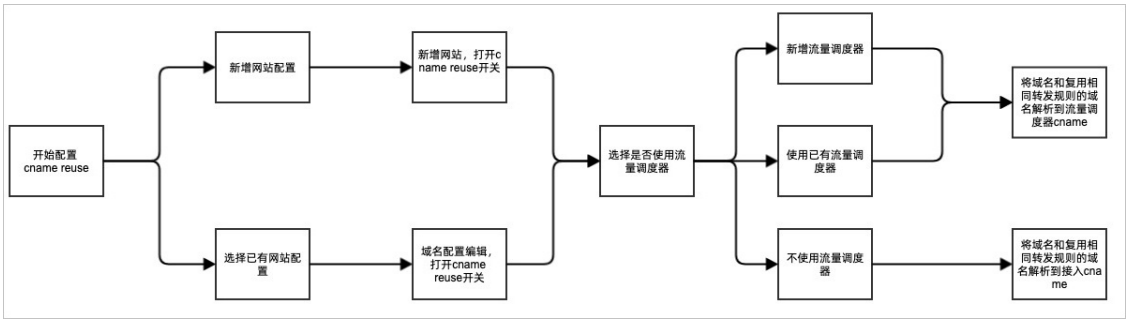
| 限制条件 | 说明 |
| --- | --- |
| 协议类型 | 支持HTTP、HTTPS协议。<br>**说明** 使用HTTPS协议接入的域名，在启用CNAME复用后，所有复用同一个CNAME地址的域名共享同一个SSL证书。 |
| 源站 | 复用CNAME的一组域名必须对应同一个源站。 |

## 开启CNAME复用

CNAME复用支持结合流量调度器使用，在开启CNAME复用时，您根据需要选择是否结合流量调度器。关于流量调度器的说明，请参见概述。

- 如果结合流量调度器使用，则需要关联对应的通用联动规则，且域名解析中将复用联动规则的CNAME地址。
- 如果不使用流量调度器，则域名解析中将复用高防网站配置的CNAME地址。

下图描述了CNAME复用的配置流程。




为便于后续操作描述，做以下假设：

- 源站服务器有两个IP：192.XX.XX.1、192.XX.XX.2。
- 源站（192.XX.XX.1）有三个域名：a.example、b.example、c.example。

以下操作描述了使用CNAME复用功能，将一个源站IP（192.XX.XX.1）下多个域名（a.example、b.example、c.example）接入DDoS防护（国际）的配置方法。

1. 在**域名接入**配置中开启Cname Reuse。
   i. 登录DDoS高防控制台。
   ii. 在顶部导航栏，选择**非中国内地**地域。
   iii. 在左侧导航栏，选择**接入管理 > 域名接入**。
   iv. 添加一个网站配置或者编辑已有网站配置，在网站配置中开启**Cname Reuse**。关于添加网站配置的具体操作，请参见添加网站。

   示例：**源站IP**设置为192.XX.XX.1，**网站**设置为a.example（也可以是b.example、c.example）。


2. 选择是否结合流量调度器及更新域名CNAME解析。

   在启用CnameReuse时，您需要选择是否使用流量调度器。具体配置方法如下：

   - 不使用流量调度器
     a. 在**选择流量调度器**对话框，选择**不使用流量调度器**，并单击**确定**。


     b. 成功添加网站配置后，记录网站配置的CNAME地址。
     c. 前往域名服务商，更新源站（192.XX.XX.1）对应的所有域名（a.example、b.example、c.example）的域名解析，应用CNAME解析并将记录值更新为网站配置的CNAME地址。
   - 使用流量调度器

a. 在**选择流量调度器**对话框，选择**使用流量调度器**，并选择对应的流量调度规则，单击**确定**。


流量调度器规则应联动网站配置中用到的源站IP（192.XX.XX.1）和DDoS高防IP。如果您还未创建对应规则，请单击**新建流量调度规则**添加对应规则（见下图示例），再选择应用规则。

> **注意** 联动规则中的DDoS高防IP必须和网站配置中关联的DDoS高防实例一致。


b. 成功选择流量调度器规则后，记录调度规则的CNAME地址。


c. 前往域名服务商，更新源站（192.XX.XX.1）对应的所有域名（a.example、b.example、c.example）的域名解析，应用CNAME解析并将记录值更新为调度规则的CNAME地址。

3. （可选）如果还需要将不同源站（例如192.XX.XX.2）对应的域名接入DDoS高防进行防护，请重复步骤1~2进行配置。

## 关闭CNAME复用

如果您不再需要使用CNAME复用，您可以在网站配置中关闭Cname Reuse。

> **警告** 关闭Cname Reuse前，请确保所有复用高防CNAME的域名已不再解析到高防，否则关闭功能后会导致网站流量转发失败。

1. 登录DDoS高防控制台。
2. 在顶部导航栏，选择**非中国内地**地域。

3. 在左侧导航栏，选择**接入管理 > 域名接入**。
4. 编辑已有网站配置，并在网站配置中关闭Cname Reuse。
5. 根据需要选择是否保留网站配置和防护调度规则：
   - 保留网站配置，则网站配置中的转发逻辑继续生效。
   - 保留防护调度规则，则流量调度器继续生效。

# 4.2. 端口接入

## 4.2.1. 添加规则

非网站业务（例如端游、手游、App等）接入DDoS高防时，您必须在DDoS高防的端口接入页面为业务添加转发规则。端口接入页面也是DDoS高防网络四层防护设置的入口，您可以根据需要为已添加的转发规则设置会话保持、健康检查、DDoS防护策略。

### 前提条件

已开通DDoS高防（新BGP）或DDoS高防（国际）实例。相关操作，请参见购买DDoS高防实例。

### 添加转发规则

1. 登录DDoS高防控制台。
2. 在顶部菜单栏左上角处，选择服务所在地域：
   - **中国内地**：选择该地域将跳转到**DDoS高防（新BGP）**控制台。
   - **非中国内地**：选择该地域将跳转到**DDoS高防（国际）**控制台。

     您可以通过切换地域分别管理和配置DDoS高防（新BGP）和DDoS高防（国际）实例。在使用DDoS高防服务时，请确认您已选择正确的地域。
3. 在左侧导航栏，选择**接入管理 > 端口接入**。
4. 在**端口接入**页面，选择要操作的DDoS高防实例，并单击**添加规则**。

> **说明** 您也可以使用批量操作添加规则，一次性添加多条规则。具体操作，请参见批量添加规则。


**转发协议**后有 图标的规则表示通过添加网站自动生成的转发规则，用来转发网站业务的流量。具体说明如下：

- 如果网站信息中的服务器端口为80，则自动生成一条转发协议为TCP、转发端口为80的转发规则。
- 如果网站信息中的服务器端口为443，则自动生成一条转发协议为TCP、转发端口为443的转发规则。

如果上述转发规则已经由其他网站配置自动生成，则再次添加网站时不会重复生成相同的转发规则。

> **说明** 通过网站配置自动生成的转发规则不支持编辑和删除，无需您进行手动操作。当使用该转发规则的所有网站配置取消与当前DDoS高防实例的关联后，自动生成的转发规则将会被自动删除。

5. 在**添加规则**对话框，根据您的实际业务情况完成规则配置，并单击**完成**。


| 参数 | 描述 |
| --- | --- |
| **转发协议** | 转发协议类型，可选值：**TCP**、**UDP**。 |
| **转发端口** | DDoS高防实例使用的转发端口。<br>**说明**<br>• 为了便于管理，建议您将**转发端口**与**源站端口**保持一致。<br>• 根据中国国家监管政策要求，为了防止未通过备案的域名业务接入防护，DDoS高防不支持80、8080、443、8443端口的端口接入配置。关于上述接口的防护，建议您使用域名接入。更多信息，请参见添加网站。<br>• 为了防止私自搭建DNS防护服务器，DDoS高防不支持53端口的端口接入配置。<br>• 不允许使用已配置的转发端口。同一DDoS高防实例和转发协议下，每条转发规则的转发端口必须唯一。当您尝试添加同协议+同转发端口的规则时，系统将提示转发规则冲突。请注意不要与通过网站配置自动生成的转发规则冲突，更多信息，请参见网站业务转发规则的说明。 |
| **源站端口** | 源站使用的业务端口。 |

| 参数 | 描述 |
| --- | --- |
| **源站IP** | 源站的IP地址。<br>**说明** 支持添加多个源站IP以实现自动负载均衡。多个IP间以半角逗号（,）分隔。最多可配置20个源站IP。 |

成功添加转发规则后，您可以在转发规则列表中查看新增的转发规则，并对转发规则执行以下操作：


- 添加**备注**：单击**转发端口**列下的

  图标，为该转发规则添加备注信息，方便您区分不同转发规则的业务场景和用途。
- 开启**会话保持**、**健康检查**，或者配置**DDoS防护策略**。

  具体操作，请参见配置转发策略。
- 编辑、删除转发规则。

  具体操作，请参见编辑规则、删除规则。
- 修改**回源设置**，为已添加的端口转发规则开启主备回源功能，增强DDoS高防回源链路的容灾能力。

  具体操作，请参见修改端口回源设置。
- 批量导出规则和防护设置。

  具体操作，请参见批量导出。

## 批量添加规则

1. 登录DDoS高防控制台。
2. 在顶部菜单栏左上角处，选择服务所在地域：
   - **中国内地**：选择该地域将跳转到**DDoS高防（新BGP）**控制台。
   - **非中国内地**：选择该地域将跳转到**DDoS高防（国际）**控制台。

     您可以通过切换地域分别管理和配置DDoS高防（新BGP）和DDoS高防（国际）实例。在使用DDoS高防服务时，请确认您已选择正确的地域。
3. 在左侧导航栏，选择**接入管理 > 端口接入**。
4. 在**端口接入**页面，选择要操作的DDoS高防实例，并单击规则列表下方的**批量操作 > 添加规则**。
5. 在**添加规则**对话框，按照格式要求填入要添加的规则配置，并单击**确定**。


规则配置的格式要求如下：

- 每行对应一条规则。
- 每条规则包含四个字段，从左到右依次是协议、转发端口、源站端口、源站IP，字段间以空格分隔。

  关于字段的含义，请参见规则配置描述。

6. 在**添加规则**对话框，选中要上传的规则，并单击**上传**。


7. 成功上传转发规则后，关闭**添加规则**对话框。

## 后续操作

添加转发规则后，您还需要执行以下操作，才能完成非网站业务的接入：

1. 在源站服务器上设置放行DDoS高防的回源IP，避免DDoS高防转发回源站的流量被源站服务器上的安全软件拦截。

   具体操作，请参见放行DDoS高防回源IP。

2. 通过本地计算机验证转发规则配置已经生效，避免转发规则配置不正确导致业务异常。

   具体操作，请参见本地验证转发配置生效。

   > **警告** 如果转发规则未生效就执行业务切换，将可能导致业务中断。

3. 将非网站业务的业务流量切换到DDoS高防实例。具体分为以下两种情况：
   - 如果您的业务直接通过IP进行访问，您只需将业务IP替换为DDoS高防实例的独享IP，即可正式将业务流量切换至DDoS高防实例。

     > **说明** 因为具体操作取决于您的业务开发平台，此处不做详细描述。

   - 如果您的业务中同时使用域名来指定服务器地址（例如，游戏客户端中设置example.com域名作为服

务器地址，或该域名已经写在客户端程序中），则您需要在域名的DNS解析服务提供商处修改DNS解析，将该域名的A记录指向DDoS高防实例的独享IP。

具体操作，请参见修改DNS解析。

# 4.2.2. 本地验证转发配置生效

成功添加DDoS高防网站或端口配置后，DDoS高防预期会把请求高防IP对应端口的报文转发到源站（真实服务器）的对应端口。为了保证业务的稳定，我们建议您在进行业务接入高防配置前先完成本地验证，确保转发配置已经生效。本文将指导您完成本地验证。

## 前提条件

- 已在DDoS高防控制台添加网站或端口配置。更多信息，请参见添加网站、添加规则。
- 已在源站服务器上设置放行DDoS高防回源IP。更多信息，请参见放行DDoS高防回源IP。

## 背景信息

对于需要通过域名访问的业务（例如客户端中使用的服务器地址是域名而不是IP），在为该类型业务接入DDoS高防时，您需要添加网站配置。添加网站配置后，您可以通过修改本地hosts文件或者使用高防CNAME地址访问服务器的方式验证转发配置生效。

有的四层业务（例如游戏业务）可能不需要域名，直接通过IP进行交互。在为该类型业务接入DDoS高防时，您需要添加端口转发规则。添加转发规则后，您可以通过使用高防IP访问服务器的方式验证转发配置生效。

> **注意** 如果转发配置未生效就执行业务切换，将可能导致业务中断。

## 修改本地hosts文件

1. 修改本地hosts文件，使本地对于被防护站点的请求经过高防。以Windows操作系统为例，操作步骤如下。
   i. 定位到hosts文件。一般hosts文件存储在*C:\Windows\System32\drivers\etc*\文件夹下。
   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`。

   例如高防IP是`180.xx.xx.173`，域名是`www.aliyundemo.com`，则在hosts文件最后一行添加的内容为`180.xx.xx.173 www.aliyundemo.com`。

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

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

   iv. 保存修改后的hosts文件。
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，请尝试刷新本地的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。

## 使用高防CNAME地址访问服务器

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

> **说明** 成功添加网站配置后，DDoS高防为域名分配一个CNAME地址，用于业务接入配置。您可以在域名接入配置列表中查看域名对应的CNAME地址。

如果无法正常访问，请确认前提条件中的配置正确。如问题依然存在，请联系阿里云售后技术支持。

### 使用高防IP访问服务器

假设高防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。

添加端口配置后，您可以直接在本地通过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。

如果本地客户端支持直接填写服务器IP，您也可以直接填入高防IP进行测试。

## 4.2.3. 修改端口回源设置

您可以通过回源设置，为已添加的端口转发规则开启主备回源功能，增强DDoS高防回源链路的容灾能力。

### 前提条件

已添加端口转发规则。相关操作，请参见添加规则。

### 背景信息

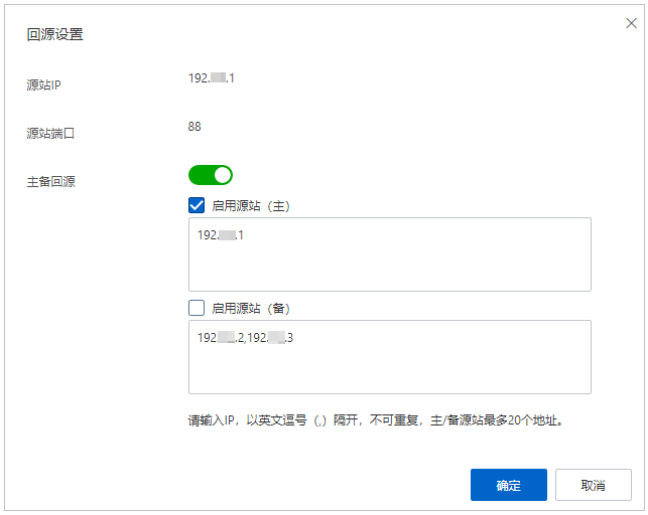
主备回源允许您预先设置主源站、备源站IP地址集合，并可随时切换选用主源站回源、备源站回源，使DDoS高防实例转发端口业务流量到您设置的主源站IP、备源站IP。当某条回源线路出现故障时，您可以快速切换到备用回源线路，确保业务访问正常。

### 开启主备回源

1. 登录DDoS高防控制台。
2. 在顶部菜单栏左上角处，选择服务所在地域：
   - **中国内地**：选择该地域将跳转到**DDoS高防（新BGP）**控制台。
   - **非中国内地**：选择该地域将跳转到**DDoS高防（国际）**控制台。

     您可以通过切换地域分别管理和配置DDoS高防（新BGP）和DDoS高防（国际）实例。在使用DDoS高防服务时，请确认您已选择正确的地域。
3. 在左侧导航栏，选择**接入管理 > 端口接入**。
4. 在转发规则列表上方，选择要操作的DDoS高防实例。
5. 定位到要设置的转发规则，单击**操作**列下的**回源设置**。


6. 在**回源设置**对话框，开启**主备回源**。




i. 打开**主备回源**开关，并在**提示**对话框单击**确定**。
开启主备回源时，默认以转发规则当前的源站IP作为主源站地址，并启用主源站回源。

ii. 设置**源站（主）**、**源站（备）**地址，并选中要启用的源站。

源站（主）、源站（备）均支持设置最多20个不同的IP地址。多个IP地址间使用半角逗号（,）分隔。

iii. 单击**确定**。

开启主备回源后，转发规则的**源站IP**将变更为您在**主备回源**中启用的源站（主、备）地址，且该转发规则不再支持**编辑**操作（即不支持通过编辑来修改转发规则的源站IP）。


后续如果您需要切换源站，只需修改转发规则的**回源设置**，选择要启用的源站（主、备）即可。

## 关闭主备回源

如果您不再需要使用主备回源功能，可以参照开启主备回源操作步骤，在**回源设置**对话框，关闭**主备回源**开关。

> **说明** 关闭主备回源后，默认以当前启用的源站（主、备）地址作为转发规则的源站IP。例如，假设当前启用了源站（备），则关闭主备回源功能后，转发规则以源站（备）地址作为源站IP，继续执行业务流量转发。

关闭主备回源后，您可以通过编辑转发规则来修改源站IP。相关操作，请参见编辑规则。

# 4.2.4. 编辑规则

您可以通过编辑转发规则，修改转发规则的源站IP。本文介绍了编辑规则和批量修改转发规则的具体操作。

## 前提条件

已经在DDoS高防实例下添加转发规则。更多信息，请参见添加规则。

## 限制说明

- 手动添加的转发规则支持修改源站IP，系统自动生成的转发规则不支持修改。
- 如果转发协议和端口发生变化，您必须添加新的转发规则。

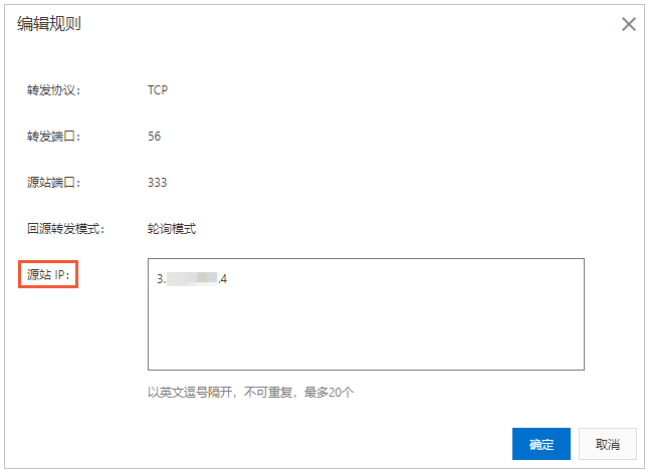
## 编辑转发规则

1. 登录DDoS高防控制台。
2. 在顶部菜单栏左上角处，选择服务所在地域：
   - **中国内地**：选择该地域将跳转到**DDoS高防（新BGP）**控制台。
   - **非中国内地**：选择该地域将跳转到**DDoS高防（国际）**控制台。

     您可以通过切换地域分别管理和配置DDoS高防（新BGP）和DDoS高防（国际）实例。在使用DDoS高防服务时，请确认您已选择正确的地域。
3. 在左侧导航栏，选择**接入管理 > 端口接入**。
4. 在**端口接入**页面，选择要操作的DDoS高防实例。
5. 定位到要编辑的转发规则，单击操作列下的**编辑**。

   > **说明** 如果您使用DDoS高防（新BGP）服务，则您也可以通过批量操作一次修改多条规则。具体操作，请参见批量修改规则。

6. 在**编辑规则**对话框，修改**源站IP**，并单击**确定**。




成功修改转发规则的源站IP后，DDoS高防会按照更新后的转发规则转发业务流量。

## 批量修改规则

> **说明** 仅DDoS高防（新BGP）服务支持批量修改规则。批量修改规则仅支持批量修改源站IP。

1. 登录DDoS高防控制台。
2. 在顶部菜单栏左上角处，选择**中国内地**地域。
   选择该地域将跳转到**DDoS高防（新BGP）**控制台。
3. 在左侧导航栏，选择**接入管理 > 端口接入**。
4. 在**端口接入**页面，选择要操作的DDoS高防实例，并在规则列表下方选择**批量操作 > 编辑规则**。


5. 在**编辑规则**对话框，按照格式要求填入要修改的规则配置，并单击**确定**。


规则配置的格式要求如下：

- 每行对应一条规则。
- 每条规则包含四个字段，从左到右依次是协议、转发端口、源站端口、源站IP（关于字段的说明，请参见规则配置描述），字段间以空格分隔。

6. 在**编辑规则**对话框，选中要上传的规则，确认后并单击**上传**。
7. 上传完成后，关闭**编辑规则**对话框。

# 4.2.5. 删除规则

对于手动添加的转发规则，如果您不再需要DDoS高防IP对业务进行转发，您必须先恢复实际业务IP，即确保实际业务没有使用高防IP，然后删除对应的转发规则。如果您未恢复实际业务IP就删除转发规则，那么可能导致业务中断。

## 前提条件

已恢复实际业务IP。

## 操作步骤

1. 登录DDoS高防控制台。
2. 在顶部菜单栏左上角处，选择服务所在地域：
   - **中国内地**：选择该地域将跳转到**DDoS高防（新BGP）**控制台。
   - **非中国内地**：选择该地域将跳转到**DDoS高防（国际）**控制台。

     您可以通过切换地域分别管理和配置DDoS高防（新BGP）和DDoS高防（国际）实例。在使用DDoS高防服务时，请确认您已选择正确的地域。
3. 在左侧导航栏，选择**接入管理 > 端口接入**。
4. 在**端口接入**页面，选择要操作的DDoS高防实例。
5. 定位到要删除的转发规则，单击其操作列下的**删除**。

> **说明** 如果要删除多条规则，您可以勾选要删除的转发规则，单击规则列表下方的**批量删除**。

6. 在删除提示对话框中，确认删除操作。

# 4.2.6. 批量导出

DDoS高防端口配置支持批量导出。您可以将DDoS高防下的全部转发规则（仅限手动添加的规则）、会话/健康配置、DDoS防护策略以txt格式导出并下载到本地。批量导出的配置格式与批量操作（例如批量添加/修改规则、批量添加会话/健康检查配置、批量添加DDoS防护策略配置）保持一致。

## 操作步骤

1. 登录DDoS高防控制台。
2. 在顶部菜单栏左上角处，选择服务所在地域：
   - **中国内地**：选择该地域将跳转到**DDoS高防（新BGP）**控制台。
   - **非中国内地**：选择该地域将跳转到**DDoS高防（国际）**控制台。

     您可以通过切换地域分别管理和配置DDoS高防（新BGP）和DDoS高防（国际）实例。在使用DDoS高防服务时，请确认您已选择正确的地域。
3. 在左侧导航栏，选择**接入管理 > 端口接入**。
4. 在**端口接入**页面，选择要操作的DDoS高防实例。
5. 在规则列表下方，根据要导出的内容类型，选择**批量导出 > 导出规则**、**批量导出 > 导出会话/健康配置**、**批量导出 > 导出DDoS防护策略**，下发相应导出任务。


6. 导出任务已下发后，单击页面右上角的任务图标。


7. 在**任务列表**页面，等待任务打包完成后，单击**下载**，下载导出文件到本地。

> **说明** 如果当前任务状态为**待执行**状态，请耐心等待导出任务完成。


成功下载导出文件到本地后，您可以打开下载的txt文件，查看规则或配置内容。关于txt文件中配置内容的格式，请参见导出格式说明。

8. （可选）在**任务列表**页面，定位到不再需要的任务，单击**删除**，将其移除。

## 导出格式说明

导出的文件均为txt格式，根据批量导出类型的不同，导出内容的格式也有区别，具体说明如下。

> **说明** 如果您使用DDoS高防（新BGP）服务，则导出文件的名称以*DDoSCoo_*开头。如果您使用DDoS高防（国际）服务，则导出文件的名称以*DDoSDip_*开头。使用DDoS高防（新BGP）和DDoS高防（国际）服务导出的内容格式相同。

- 规则文件

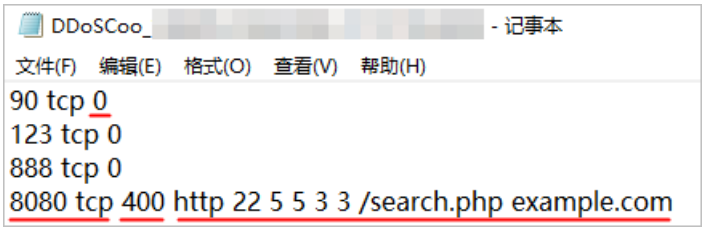
  每行对应一条规则，每条规则包含四个字段，从左到右依次是协议、转发端口、源站端口、源站IP。

  更多信息，请参见添加规则。

- 会话/健康配置文件

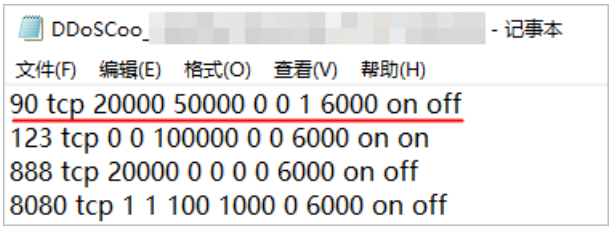
  每行对应一个规则的配置，每条配置包含以下字段（从左到右）：转发协议端口、转发协议、会话保持超时时间（若为0则表示未开启会话保持）、健康检查类型（若为空则表示未开启健康检查，且后续字段均为空）、检查端口、检查超时时间、检查间隔、不健康阈值、健康阈值、检查路径（HTTP类型下存在）、域名（HTTP类型下存在）。




更多信息，请参见配置会话保持。

- DDoS防护策略文件

  每行对应一个规则的配置，每条配置包含以下字段（从左到右）：转发协议端口、转发协议、源新建连接限速、源并发连接限速、目的新建连接限速、目的并发连接限速、包长度最小值、包长度最大值、虚假源与空连接（仅TCP协议时生效，空连接开启前需要先开启虚假源）。




更多信息，请参见批量添加DDoS防护策略。

# 4.2.7. 配置健康检查

DDoS高防为已接入防护的非网站业务提供网络四层和七层健康检查功能，适用于业务有多个源站IP时，判断后端服务器的业务可用性。在DDoS高防实例下添加端口转发规则后，您可以为转发规则开启健康检查。

## 前提条件

- 已在端口接入中配置非网站业务端口转发规则。

  更多信息，请参见添加规则。

- 端口转发规则中配置了多个源站IP地址。

> 注意　如果在端口转发规则中仅配置了一个源站IP，请不要开启健康检查。

## 背景信息

健康检查适用于配置了多个源站IP的业务。DDoS高防在转发业务流量回源时，通过健康检查判断源服务器的业务可用性，将流量优先转发到状态健康的源服务器，保证业务正常响应。更多信息，请参见负载均衡健康检查概述。

## 开启健康检查

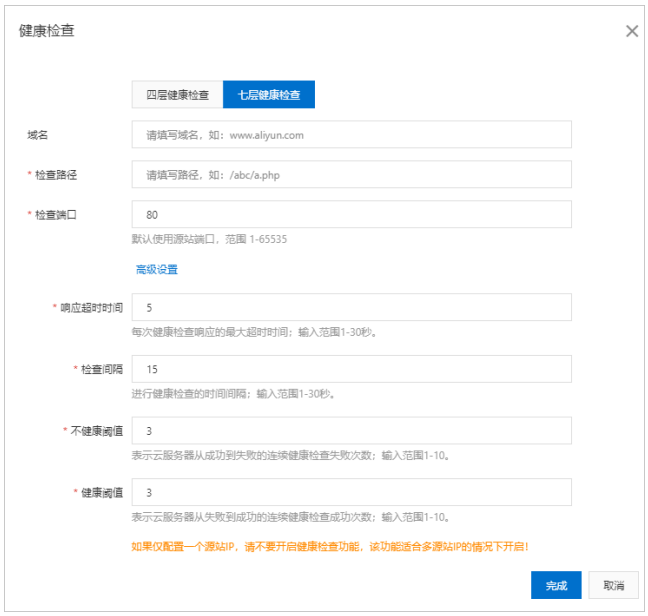
1. 登录DDoS高防控制台。
2. 在顶部菜单栏左上角处，选择服务所在地域：
   - **中国内地**：选择该地域将跳转到**DDoS高防（新BGP）**控制台。
   - **非中国内地**：选择该地域将跳转到**DDoS高防（国际）**控制台。

     您可以通过切换地域分别管理和配置DDoS高防（新BGP）和DDoS高防（国际）实例。在使用DDoS高防服务时，请确认您已选择正确的地域。

3. 在左侧导航栏，选择**接入管理 > 端口接入**。
4. 在**端口接入**页面，选择DDoS高防实例，并定位到要操作的转发规则，单击**健康检查**列下的**配置**。

> **说明** 您也可以在DDoS高防实例下使用批量操作，批量修改会话保持和健康检查配置。具体操作，请参见批量添加会话和健康检查配置。


5. 在**健康检查**对话框，完成健康检查配置，并单击**完成**。




DDoS高防支持网络四层和七层健康检查配置，具体参数描述如下表所示。

> **说明** 四层健康检查和七层健康检查均支持高级设置。高级设置仅在展开**高级设置**后显示。一般情况下，建议您不要修改高级设置。

| 类型 | 参数 | 说明 |
| --- | --- | --- |
| **四层健康检查** | **检查端口** | 健康检查服务访问后端服务器时的探测端口。取值范围：1~65535。默认值为配置监听时指定的后端端口。<br>**说明** 适用于TCP和UDP协议规则。 |

| 类型 | 参数 | 说明 |
| --- | --- | --- |
| 七层健康检查 | 域名、检查路径 | 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。<br>说明 仅适用TCP协议规则（HTTP业务）。<br>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。<br>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。 |
| | 检查端口 | 健康检查服务访问后端服务器时的探测端口。取值范围：1~65535。默认值为配置监听时指定的后端端口。 |
| 高级设置 | 响应超时时间 | 每次健康检查响应的最大超时时间。取值范围：1~30，单位：秒。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。取值范围：1~30，单位：秒。<br>说明 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，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。取值范围：1~10，单位：次。 |
| | 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。取值范围：1~10，单位：次。 |

成功开启健康检查后，端口转发规则的**健康检查**状态更新为**已开启**。


## 批量添加会话和健康检查配置

1. 登录DDoS高防控制台。
2. 在顶部菜单栏左上角处，选择服务所在地域：
   - **中国内地**：选择该地域将跳转到**DDoS高防（新BGP）**控制台。
   - **非中国内地**：选择该地域将跳转到**DDoS高防（国际）**控制台。

     您可以通过切换地域分别管理和配置DDoS高防（新BGP）和DDoS高防（国际）实例。在使用DDoS高防服务时，请确认您已选择正确的地域。
3. 在左侧导航栏，选择**接入管理 > 端口接入**。

4. 在**端口接入**页面，选择要操作的DDoS高防实例，并在规则列表下方选择**批量操作 > 添加会话/健康检查配置**。


5. 在**添加会话/健康检测配置**对话框，按照格式要求输入要添加的会话保持和健康检查配置内容，并单击**确定**。


> **说明** 您也可以先批量导出当前会话和健康检查配置，在导出的TXT文件中统一调整后再将内容复制粘贴进来。更多信息，请参见批量导出。

会话保持、健康检查配置的格式要求如下：

- 每行对应一条转发规则的会话保持和健康配置。
- 每条会话保持和健康检查配置从左到右包含以下字段：转发协议端口、转发协议（取值：TCP、HTTP、UDP）、会话保持超时时间（单位：秒，取值范围：30~3600）、健康检查类型、检查端口、检查超时时间、检查间隔、不健康阈值、健康阈值、检查路径（转发协议为HTTP时必选）、域名（转发协议为HTTP时可选）。字段间以空格分隔。
- 转发协议端口必须是已添加规则的端口。
- 转发规则协议为UDP时，建议配置UDP健康检查。转发规则协议为TCP时，建议配置TCP（四层）或HTTP（七层）健康检查。
- 转发协议为HTTP时，检查路径必选，域名可选。

# 4.2.8. 配置会话保持

如果您的非网站业务接入DDoS高防后存在登录超时需要重新登录、上传数据断开等问题，您可以开启会话保持功能。会话保持可以在指定的时间范围内将同一客户端的请求转发至同一台后端服务器上。本文介绍了为端口转发规则配置会话保持的方法。

## 前提条件

已在端口接入中配置非网站业务端口转发规则。更多信息，请参见添加规则。

## 开启会话保持

1. 登录DDoS高防控制台。
2. 在顶部菜单栏左上角处，选择服务所在地域：
   - **中国内地**：选择该地域将跳转到**DDoS高防（新BGP）**控制台。
   - **非中国内地**：选择该地域将跳转到**DDoS高防（国际）**控制台。

     您可以通过切换地域分别管理和配置DDoS高防（新BGP）和DDoS高防（国际）实例。在使用DDoS高防服务时，请确认您已选择正确的地域。
3. 在左侧导航栏，选择**接入管理 > 端口接入**。
4. 在**端口接入**页面，选择DDoS高防实例，并定位到要操作的转发规则，单击**会话保持**列下的**配置**。

   > **说明** 您也可以在高防实例下使用批量操作，批量修改会话和健康检查配置。具体操作，请参见批量添加会话和健康检查配置。


5. 在**会话保持**对话框，设置**超时时间**（单位：秒，取值范围：30~3600），并单击**设置超时时间并开启**。


成功开启会话保持后，转发规则的**会话保持**状态会更新为**已开启**。


## 批量添加会话和健康检查配置

1. 登录DDoS高防控制台。
2. 在顶部菜单栏左上角处，选择服务所在地域：
   - **中国内地**：选择该地域将跳转到**DDoS高防（新BGP）**控制台。
   - **非中国内地**：选择该地域将跳转到**DDoS高防（国际）**控制台。

     您可以通过切换地域分别管理和配置DDoS高防（新BGP）和DDoS高防（国际）实例。在使用DDoS高防服务时，请确认您已选择正确的地域。

3. 在左侧导航栏，选择**接入管理 > 端口接入**。
4. 在**端口接入**页面，选择要操作的DDoS高防实例，并在规则列表下方选择**批量操作 > 添加会话/健康检查配置**。


5. 在**添加会话/健康检测配置**对话框，按照格式要求输入要添加的会话保持和健康检查配置内容，并单击**确定**。


> **说明** 您也可以先批量导出当前会话和健康检查配置，在导出的TXT文件中统一调整后再将内容复制粘贴进来。更多信息，请参见批量导出。

会话保持、健康检查配置的格式要求如下：

- 每行对应一条转发规则的会话保持和健康配置。
- 每条会话保持和健康检查配置从左到右包含以下字段：转发协议端口、转发协议（取值：TCP、HTTP、UDP）、会话保持超时时间（单位：秒，取值范围：30~3600）、健康检查类型、检查端口、检查超时时间、检查间隔、不健康阈值、健康阈值、检查路径（转发协议为HTTP时必选）、域名（转发协议为HTTP时可选）。字段间以空格分隔。
- 转发协议端口必须是已添加规则的端口。
- 转发规则协议为UDP时，建议配置UDP健康检查。转发规则协议为TCP时，建议配置TCP（四层）或HTTP（七层）健康检查。
- 转发协议为HTTP时，检查路径必选，域名可选。

# 4.3. 业务接入配置

## 4.3.1. 修改DNS解析接入网站业务

在DDoS高防添加网站配置后，您必须将网站域名的DNS解析记录修改为高防CNAME地址或IP，才能使用户访问网站的流量切换到DDoS高防实例进行防护。本文以网站域名解析托管在阿里云云解析DNS（免费版）为例，介绍了手动修改域名解析（CNAME或A记录）以接入DDoS高防的操作方法。

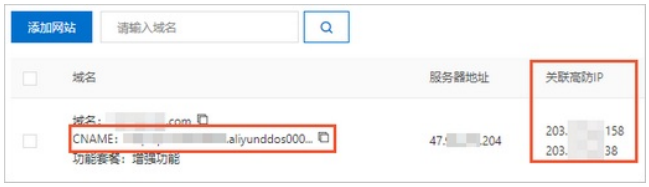
## 前提条件

- 网站已接入DDoS高防。更多信息，请参见添加网站。
- 源站服务器已放行DDoS高防回源IP。如果您的源站服务器上部署了非阿里云安全软件（例如，第三方防火墙），请将DDoS高防的回源IP地址加入安全软件的白名单，避免DDoS高防的回源流量被源站服务器上的安全软件误拦截。更多信息，请参见放行DDoS高防回源IP。
- 验证转发配置生效。强烈建议您在切换网站访问流量前，在本地验证DDoS高防实例的业务转发配置已经生效。更多信息，请参见本地验证转发配置生效。

> **警告** 如果转发配置未生效就执行业务切换，将可能导致业务中断。

## 接入方式说明

手动修改DNS解析接入网站业务时，您可以选择将网站域名的解析指向高防CNAME地址或关联高防IP（网站域名的高防CNAME地址和关联高防IP地址均可在DDoS高防控制台的**接入管理 > 域名接入**页面查询）。




接入方式的区别如下：

- 使用CNAME解析接入DDoS高防，只需完成一次解析修改，即使后续网站的关联高防IP发生变化，无需重新修改解析，DDoS高防将通过CNAME自动完成调度。在网站关联多个高防IP时，DDoS高防自动在多IP间切换流量。
- 使用A记录解析接入，则当网站的关联高防IP发生变化时，您必须重新修改解析。在网站关联多个高防IP时，您必须手动在多IP间切换流量。

我们推荐您使用CNAME方式接入，仅在CNAME解析不被支持或与别的记录存在冲突时，再选择A记录方式接入。

## 操作步骤

以下操作描述建立在您的域名DNS托管在阿里云云解析DNS的前提下。

> **说明** 云解析DNS是阿里云提供的域名解析服务，支持免费的公共DNS服务和付费版增值服务。如果您的域名已开通付费版云解析DNS服务，我们推荐您使用NS接入（即自动修改DNS）的方式接入DDoS高防。更多信息，请参见NS方式接入网站业务。

如果您使用其他DNS服务商的域名解析服务，请登录服务商系统修改网站域名的解析记录，下文内容仅供参考。

假设在DDoS高防控制台已添加网站的域名为 `bgp.aliyundoc.com` 。以下操作示例描述了在云解析DNS控制台修改、新增域名解析的步骤。

1. 登录阿里云云解析DNS控制台。
2. 在**域名解析**页面，定位到要操作的域名（本示例中为 `aliyundoc.com` ），单击**操作**列下的**解析设置**。
3. 在**解析设置**页面，定位到要修改的解析记录（本示例中对应主机记录为**bgp**的A记录或CNAME记录），单击**操作**列下的**修改**。

> **说明** 如果要操作的解析记录不在记录列表中，您可以单击**添加记录**。


4. 在**修改记录**（或**添加记录**）页面，选择一种接入方式，修改解析记录。
   - （推荐）CNAME解析接入：选择**记录类型**为**CNAME**，并将**记录值**修改为域名对应的DDoS高防CNAME地址。

     > **说明** 您可以在DDoS高防控制台的**接入管理** > **域名接入**页面查询域名对应的DDoS高防CNAME地址。

   - A记录解析接入：选择**记录类型**为**A**，并将**记录值**修改为域名的关联高防IP。

     > **说明** 您可以在DDoS高防控制台的**接入管理** > **域名接入**页面查询域名的关联高防IP。

5. 单击**确认**，等待修改后的解析设置生效。
6. 使用浏览器测试网站访问是否正常。

   如果网站访问出现异常，请参见业务接入高防后存在卡顿、延迟、访问不通等问题。

## 相关操作

业务接入DDoS高防后，您可以根据需要完成以下任务：

- 启用流量调度器，设置DDoS高防与云资源间的联动规则，仅在特定场景下触发并切换启用DDoS高防。更多信息，请参见概述。
- 更换源站ECS公网IP。如果您的源站IP不慎暴露，攻击者有可能绕过高防直接攻击源站，这种情况下，您可以通过DDoS高防更换后端ECS的IP。更多信息，请参见更换源站ECS公网IP。

# 4.3.2. NS方式接入网站业务

网站业务接入DDoS高防时，您在网站配置中添加网站，然后修改网站域名的DNS解析，将业务流量切换到DDoS高防实例进行防护。开启NS方式接入帮助您自动修改域名DNS解析，但前提是您的域名解析托管在阿里云云解析DNS且已开通云解析DNS付费版服务。本文介绍了使用NS接入的操作方法。

## 前提条件

- 已开通DDoS高防（新BGP）实例。

  > **说明** 目前仅DDoS高防（新BGP）服务支持NS接入，如果您使用DDoS高防（国际）服务，建议您使用修改DNS解析的方式接入DDoS高防。更多信息，请参见修改DNS解析接入网站业务。

- 网站域名的DNS解析托管在阿里云云解析DNS，且已开通云解析DNS付费版。更多信息，请参见云解析DNS产品详情。
- 网站已接入DDoS高防。更多信息，请参见添加网站。
- 源站服务器已放行DDoS高防回源IP。如果您的源站服务器上部署了非阿里云安全软件（例如，第三方防火墙），请将DDoS高防的回源IP地址加入安全软件的白名单，避免DDoS高防的回源流量被源站服务器上的安全软件误拦截。更多信息，请参见放行DDoS高防回源IP。

- 验证转发配置生效。强烈建议您在切换网站访问流量前，在本地验证DDoS高防实例的业务转发配置已经生效。更多信息，请参见本地验证转发配置生效。

  警告 如果转发配置未生效就执行业务切换，将可能导致业务中断。

## 背景信息

开启NS方式接入后，DDoS高防将依据网站配置中的转发信息，自动更新云解析DNS中的解析记录，实现业务流量的简便切换。NS方式支持以下两种工作模式：

- DDoS高防模式：将业务流量牵引到DDoS高防，即开启DDoS防护。


- 回源模式：将业务流量直接指回源站，即关闭DDoS防护。


下文描述了开启和配置NS方式接入的具体操作。如果因为特殊情况无法使用NS方式（例如域名解析托管在其他DNS解析服务商且不方便迁移等），请通过手动修改DNS解析的方式接入网站业务。更多信息，请参见修改DNS解析接入网站业务。

## 操作步骤

1. 登录DDoS高防控制台。
2. 在顶部导航栏，选择**中国内地**地域。
3. 在左侧导航栏，选择**接入管理 > 域名接入**。
4. 在**域名接入**页面，定位到要操作的域名，单击其操作列下的**DNS设置**。


5. 在**DNS设置**页面，定位到**NS方式接入**模块，开启**状态**开关并选择一种接入模式：**DDoS高防**、**回源**。
   - DDoS高防模式：自动更新云解析DNS配置，将当前域名的解析目标指向DDoS高防实例。
   - 回源模式：自动更新云解析DNS配置，将当前域名的解析目标指向源站。


   如果当前阿里云账号已开通云解析DNS付费版服务，开关将正常开启。如果未开通云解析DNS付费版服务，将提示无法使用NS方式。
6. 完成配置后，等待域名解析生效。您可以通过第三方DNS测试平台检测该域名的最新解析结果是否符合预期。

# 4.3.3. CNAME解析接入非网站业务

非网站（四层）业务接入DDoS高防时，您在端口配置中添加转发规则，并将业务地址设置为高防IP即可。但在某些场景下，您可能需要用域名来接入四层业务，并实现业务关联多高防IP且多高防IP间自动切换流量。这种情况下，推荐您通过添加域名并修改CNAME解析来接入非网站业务。

## 背景信息

假设您要为游戏业务接入DDoS高防，并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IP（也就是DDoS高防IP），游戏的TCP端口为1234和5678，源站为1.1.1.1。

## 操作步骤

1. 在网站配置中添加网站，获取CNAME地址。
   i. 登录DDoS高防控制台。
   ii. 在顶部导航栏，选择服务所在地域：
      - **中国内地**：DDoS高防（新BGP）服务
      - **非中国内地**：DDoS高防（国际）服务
   iii. 在左侧导航栏，单击**接入管理 > 域名接入**。
   iv. 在**域名接入**页面，单击**添加网站**。

v. 在**添加网站**页面，完成**填写网站信息**任务，并单击**添加**。

要添加的配置描述如下：

- **功能套餐**和**实例**：选择要关联的DDoS高防实例。本示例中假设关联增强功能下的两个实例。
- **网站**：填写业务域名。本示例中是game.aliyundemo.com。
- **协议类型**和**服务器端口**：保持默认。
- **服务器地址**：选择**源站IP**，并根据实际情况填写。
  - 如果业务域名下有真实的网站业务，则必须提供正确的协议类型和源站IP。
  - 否则，您可以随意填写源站IP，因为该网站配置不用于实际业务转发。实际业务转发通过在步骤2中添加的端口转发规则实现。

更多信息，请参见添加网站。

成功添加网站后，DDoS高防为域名分配一个CNAME地址。


2. 在端口配置中添加转发规则。

i. 在左侧导航栏，单击**接入管理 > 端口接入**。

ii. 在**端口接入**页面，选择要操作的DDoS高防IP，并单击**添加规则**。

> **说明** 此处的DDoS高防IP即步骤1为域名关联的高防IP。本示例中有两个，选择其中任意一个。

iii. 在**添加规则**对话框，根据您的实际业务情况完成规则配置，并单击**完成**。

要添加的配置描述如下：

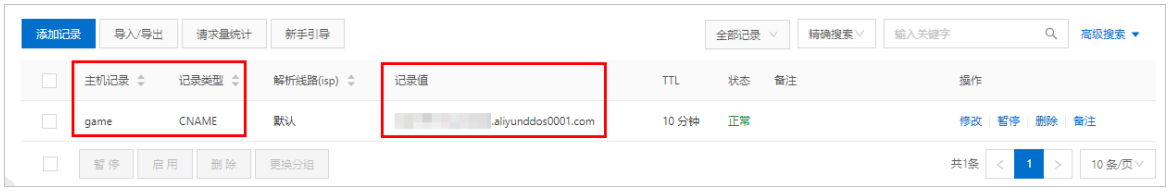
- **转发协议**：本示例中选择TCP。
- **转发端口**：本示例中填写1234。
- **源站端口**：本示例中填写1234。
- **源站IP**：填写真实源站IP，本示例中是1.1.1.1。

更多信息，请参见添加规则。

iv. 重复上述两个步骤，在当前DDoS高防IP下再添加一个转发规则，将转发端口和源站端口设置为5678。


v. 参照上述三个步骤，为其他DDoS高防IP配置同样的转发规则。


3. 前往域名（game.aliyundemo.com）的DNS解析服务商，手动修改域名的DNS解析，启用CNAME解析并将解析指向步骤1中获得的CNAME地址。




更多信息，请参见修改DNS解析接入网站业务。

# 4.3.4. 修改CNAME解析接入流量调度器

通过流量调度器添加调度规则后，您必须更新域名的DNS解析（CNAME记录），将网站业务流量切换至流量调度器，才能使调度规则生效。本文以网站域名解析托管在阿里云云解析DNS为例，介绍了手动修改域名解析（CNAME记录）以接入流量调度器的操作方法。

## 前提条件

已通过流量调度器添加调度规则。更多信息，请参见概述。

## 背景信息

通过流量调度器添加调度规则后，流量调度器会为规则生成一个CNAME地址。修改CNAME解析接入流量调度器时，您需要将网站域名的解析（CNAME记录）设置为流量调度器生成的CNAME地址。

以下操作描述建立在您的域名DNS托管在阿里云云解析DNS的前提下。

如果您使用其他DNS服务商的域名解析服务，请登录服务商系统修改网站域名的解析记录，下文内容仅供参考。

假设调度规则对应的网站域名为 `bgp.gftest.top` 。以下操作示例描述了在云解析DNS控制台修改、新增域名解析的具体操作。

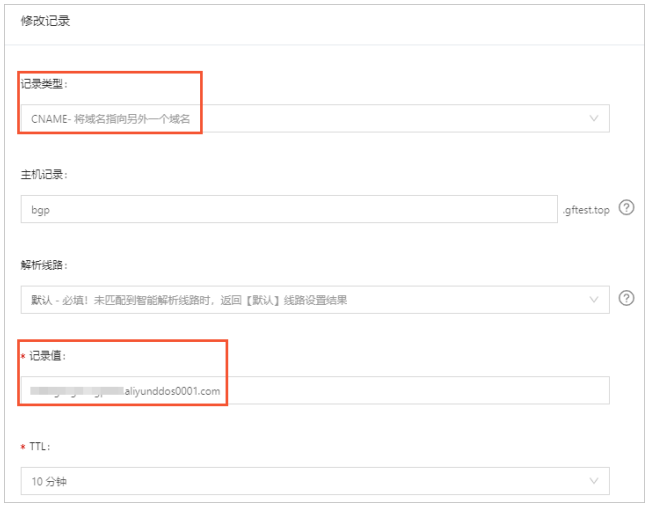
## 操作步骤

1. 登录阿里云云解析DNS控制台。
2. 在**域名解析**页面，定位到要操作的域名（本示例中为 `aliyundoc.com` ），单击**操作**列下的**解析设置**。
3. 在**解析设置**页面，定位到要修改的解析记录（本示例中对应主机记录为**bgp**的A记录或CNAME记录），单击**操作**列下的**修改**。

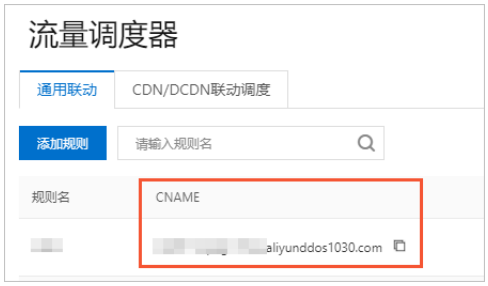
   > **说明** 如果要操作的解析记录不在记录列表中，您可以单击**添加记录**。

4. 在**修改记录**（或**添加记录**）对话框，选择**记录类型**为**CNAME**，并将**记录值**修改为流量调度器的CNAME地址。

   您可以登录DDoS高防控制台，在**接入管理 > 流量调度器**页面，查询流量调度器的CNAME地址。

5. 单击**确认**，等待修改后的解析设置生效。
6. 使用浏览器测试网站访问是否正常。

   如果网站访问出现异常，请参见业务接入高防后存在卡顿、延迟、访问不通等问题。

# 4.4. 流量调度器

# 4.4.1. 概述

流量调度器支持设置DDoS高防和云资源间的联动规则，仅在特定场景下触发并切换启用DDoS高防，保证无DDoS攻击时日常业务流畅运行、发生DDoS攻击时可切换至DDoS高防，为您的业务提供防护。流量调度器包括云产品联动、阶梯防护、CDN/DCDN联动、出海加速、安全加速场景。

## 是否使用流量调度器有什么区别？

在将业务接入DDoS高防进行防护时，您只需完成域名接入（适合网站类业务，详见添加网站）或端口接入（适合非网站类业务，详见添加规则）即可，无需使用流量调度器。

业务正常接入DDoS高防后，所有业务流量（包括正常访问和发生攻击）都经过DDoS高防转发，其中攻击流量被清洗，只有正常访问流量被转发到源站服务器。在业务正常访问期间，由于正常业务流量也都经过DDoS高防转发，会给业务带来少量延迟。

针对业务正常访问期间的延迟问题，您可以开启流量调度器的云产品联动功能，实现正常业务访问期间流量不经过高防转发，直接达到源站服务器，不增加延迟；仅在业务被攻击时切换到高防进行流量转发，帮助业务清洗DDoS攻击。

除了上述场景外，流量调度器还能实现DDoS高防与DDoS原生防护、CDN或DCDN、加速线路、安全加速线路的联动使用，具体请参见联动场景。

> **说明** 流量调度器是DDoS高防提供的一项接入设置功能，是否使用流量调度器和服务计费没有关系。关于DDoS高防的计费方式，请参见DDoS高防（新BGP）计费方式、保险版和无忧版计费方式。

## 联动场景

下表介绍了DDoS高防流量调度器的不同联动场景和相关文档。

×表示DDoS高防（新BGP）实例不支持的联动场景。

| 联动场景 | 说明 | DDoS高防（新BGP） | DDoS高防（国际） |
| --- | --- | --- | --- |
| **云产品联动** | 业务使用**阿里云公网IP资源**且接入**DDoS高防**进行防护，实现以下效果：<br>• 无攻击时，业务流量直达源站服务器，高防做备用，不增加延迟。<br>• 被攻击时，自动切换至DDoS高防，业务流量经过DDoS高防转发。<br>**说明** 支持与阿里云全球加速实例联动，详见什么是全球加速。 | 云产品联动 | |
| **阶梯防护** | 业务同时接入**DDoS原生防护企业版**和**DDoS高防**进行防护，实现以下效果：<br>• 使用原生防护企业版抵御日常攻击，业务流量直达源站服务器，不增加延迟。<br>• 发生大流量攻击时，切换至DDoS高防进行防护，业务流量经过DDoS高防转发。 | 阶梯防护 | |

| 联动场景 | 说明 | DDoS高防（新BGP） | DDoS高防（国际） |
| --- | --- | --- | --- |
| **CDN/DCDN联动调度** | 网站业务开启了**阿里云CDN或DCDN**加速服务，且接入**DDoS高防**进行防护，实现以下效果：<br>• 无攻击时，就近使用CDN或DCDN节点加速。<br>• 被攻击时，切换至DDoS高防进行防护。 | CDN/DCDN联动调度 | |
| **出海加速** | 业务同时接入**DDoS高防（国际）保险版或无忧版**和**加速线路**，实现以下效果：<br>• 无攻击时，业务流量经过加速线路IP，提升访问速度。<br>• 被攻击时，切换至DDoS高防（国际）进行防护。<br>**说明** 出海加速方案适用于业务服务器部署在中国内地以外地域，但主要用户来自中国内地的场景，详见配置DDoS高防（国际）加速线路。 | × | 出海加速 |
| **安全加速** | 业务同时接入**DDoS高防（国际）保险版或无忧版**和**安全加速线路**，实现以下效果：<br>• 中国电信和联通以及非移动运营商流量调度到安全加速线路对应的IP上。<br>• 中国移动和海外流量调度到DDoS高防（国际）对应的IP上。<br>**说明** 安全加速线路适用于中国内地地区用户对非中国内地业务加速访问的同时，还可以为中国电信、联通和非移动线路提供大流量DDoS攻击防护能力，详见配置DDoS高防（国际）安全加速。 | × | 添加安全加速规则 |

# 4.4.2. 云产品联动

云产品联动表示通过自定义规则，联动使用DDoS高防与阿里云公网IP资源，解决网站业务接入高防防护后，正常业务访问延时增加的问题。

## 前提条件

- 业务使用阿里云公网IP资源，具体包括拥有公网IP的云服务器ECS或负载均衡SLB、弹性公网IP、Web应用防火墙。
- 已购买DDoS高防（新BGP）专业版实例、DDoS高防（国际）保险版或无忧版实例。

  **注意** DDoS高防实例的业务带宽、QPS等规格必须满足正常业务防护需求。

  相关操作，请参见购买DDoS高防实例。
- 已将网站业务接入DDoS高防实例进行防护。

  相关操作，请参见添加网站。
- 已验证DDoS高防实例可以正常转发业务流量。

相关操作，请参见本地验证转发配置生效。

## 背景信息

业务接入DDoS高防防护后，默认所有业务流量都经过DDoS高防转发，其中攻击流量被清洗后丢弃，只有正常业务流量被转发到源站服务器。在业务正常访问期间（无攻击时），由于正常业务流量也经过DDoS高防转发，会给业务访问带来少量延迟。

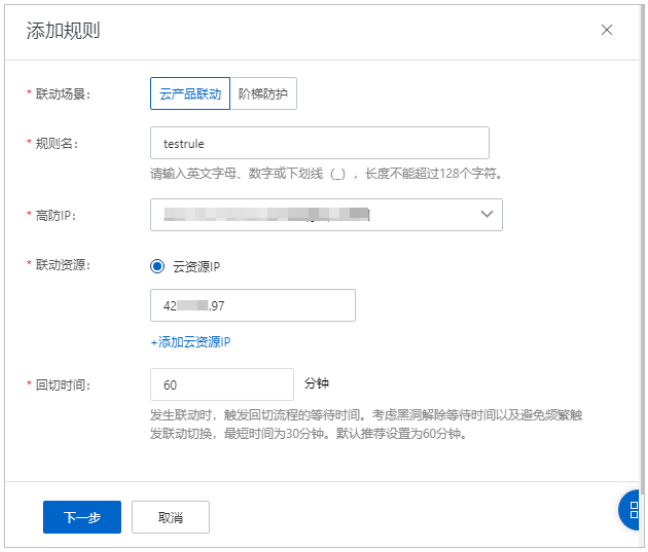
如果您希望在业务正常访问期间不增加延迟，则可以通过流量调度器创建一条云产品联动调度规则，实现业务正常访问期间，流量直达源站服务器（不增加延时）；仅在业务被攻击时，流量切换到DDoS高防，经清洗后再转发到源站服务器。

## 添加云产品联动规则

1. 登录DDoS高防控制台。
2. 在顶部菜单栏左上角处，选择服务所在地域：
   - **中国内地**：选择该地域将跳转到**DDoS高防（新BGP）**控制台。
   - **非中国内地**：选择该地域将跳转到**DDoS高防（国际）**控制台。

     您可以通过切换地域分别管理和配置DDoS高防（新BGP）和DDoS高防（国际）实例。在使用DDoS高防服务时，请确认您已选择正确的地域。
3. 在左侧导航栏，选择**接入管理 > 流量调度器**。
4. 在**通用联动**页签，单击**添加规则**。
5. 在**添加规则**面板，配置**云产品联动**规则，并单击**下一步**。

   DDoS高防（新BGP）云产品联动规则示例




| 参数 | 描述 |
| --- | --- |
| **联动场景** | 选择**云产品联动**。 |
| **规则名** | 为规则命名。<br>规则名由英文字母、数字和下划线（_）组成，不超过128个字符。 |
| **高防IP** | 选择要联动的DDoS高防实例。 |

| 参数 | 描述 |
| --- | --- |
| **联动资源** | 输入要联动的**云资源IP**，可以使用ECS实例IP、SLB实例IP、WAF实例IP、EIP。<br>单击**添加云资源IP**，可以添加多个云资源。最多支持添加20个IP。<br>**说明** 添加多个云资源IP时（即多个云资源IP关联一个高防IP），如果一个云资源IP上发生DDoS攻击，将优先使用其他云资源IP，直到无可用云资源IP时，才会切换到高防进行防护。如果您希望云产品多路分摊流量，每路被攻击时单独切换高防，请参见多路分摊切换配置。 |
| **回切时间** | 业务流量联动到DDoS高防进行防护后，允许触发回切流程（切换回云资源IP）的等待时间。攻击结束且经过该等待时间后，业务流量自动回切到云资源IP。<br>可选范围：30~120分钟。推荐您设置为60分钟。 |

6. 按照页面提示修改域名的DNS解析设置，并单击**完成**。

   要使联动规则生效，您必须在域名的DNS服务商处修改域名的DNS解析（如果域名通过阿里云域名服务注册，只需在云解析DNS控制台操作；否则需要在注册域名的第三方平台操作），将解析指向流量调度器的CNAME地址。

   **注意** 您修改域名的DNS解析后，流量调度规则将会生效。建议您在修改DNS解析前，先通过修改本地计算机的*hosts*文件配置，验证流量调度规则，避免因回源策略不一致出现不兼容问题。例如，在CDN和高防联动且回源到OSS的场景，由于CDN回源支持修改回源HOST，而DDoS高防不支持，导致发生攻击自动切换到DDoS高防后，DDoS高防回源到OSS的正常流量无法被识别，出现业务故障。

   关于验证流量调度规则的操作，请参见本地验证转发配置生效。

   关于修改域名DNS解析的操作，请参见修改CNAME解析接入流量调度器。

配置云产品联动规则后，如果云资源上未发生DDoS攻击，业务流量不经过DDoS高防清洗，直接由客户端到云资源；只有在云资源上发生DDoS攻击时，业务流量才会自动切换到DDoS高防进行清洗，保证只有正常业务流量会转发到云资源。业务流量自动切换到DDoS高防后，DDoS高防将在攻击结束后等待一段时间（**回切时间**），自动将业务流量回切到云资源。

除了自动切换方式，您还可以选择手动切换，即根据业务防护需求，手动将业务流量切换到DDoS高防进行清洗、回切到云资源。更多信息，请参见相关操作。

## 相关操作

成功添加通用联动规则后，您可以在规则列表，对已添加的规则执行以下操作。

| 操作 | 说明 |
| --- | --- |

| 操作 | 说明 |
| --- | --- |
| **切到高防** | 在未自动触发DDoS高防清洗（**联动资源**下有<br>●<br>图标）时，手动将业务流量切换到DDoS高防进行清洗。适用于在业务触发黑洞前提前切换，减少业务损伤。<br>  <br><br>只有当DDoS高防IP不在黑洞中，才可以正常切换到DDoS高防。<br>**注意** 手动将业务流量切换到DDoS高防后，默认不会自动回切到联动资源。如需回切到联动资源，您必须手动执行**回切**操作。 |
| **回切** | 在业务流量由DDoS高防清洗（**高防IP**下有<br>●<br>图标）时，手动将业务流量回切到联动资源。<br>  <br><br>**注意**<br>• 建议您在执行回切前，确认攻击已经结束并且回切的联动资源线路可用，避免联动资源处于沙箱状态导致业务中断。<br>• 如果您通过**切到高防**操作将业务流量切换到DDoS高防，则只能通过**回切**操作将流量回切到联动资源。<br>如果联动资源全部在黑洞中，回切操作将会失败。如果有部分联动资源已经解除黑洞，部分联动资源还在黑洞中，流量将先回切到已经解除黑洞的联动资源上，其他资源等待黑洞解除后自动恢复流量。 |
| **编辑** | 编辑通用联动规则，修改除**联动场景**、**规则名**以外的参数配置。 |
| **删除** | 删除通用联动规则。<br>**警告** 删除联动规则前，请确保网站域名的解析没有指向流量调度器CNAME，否则删除联动规则后，网站将无法正常访问。 |

# 4.4.3. 阶梯防护

阶梯防护表示通过自定义规则，联动使用DDoS高防与DDoS原生防护企业版服务，解决网站业务接入高防防护后，正常业务访问延时增加的问题。阶梯防护可实现由DDoS原生防护防御日常攻击（不增加延时），仅在发生大流量攻击时切换到DDoS高防进行防护。

## 前提条件

- 业务使用阿里云公网IP资源，具体包括拥有公网IP的云服务器ECS或负载均衡SLB、弹性公网IP、Web应用防火墙。
- 已购买DDoS原生防护企业版实例，并为云资源IP（ECS、SLB、EIP、WAF）开启了DDoS原生防护。

  > 注意　DDoS原生防护企业版实例的地域必须与云资源的地域一致。

  相关操作，请参见购买DDoS原生防护企业版实例、添加防护对象。
- 已购买DDoS高防（新BGP）专业版实例、DDoS高防（国际）保险版或无忧版实例。

  > 注意　DDoS高防实例的业务带宽、QPS等规格必须满足正常业务防护需求。

  相关操作，请参见购买DDoS高防实例。
- 已将网站业务接入DDoS高防实例进行防护。

  相关操作，请参见添加网站。
- 已验证DDoS高防实例可以正常转发业务流量。

  相关操作，请参见本地验证转发配置生效。

## 添加阶梯防护联动规则

1. 登录DDoS高防控制台。
2. 在顶部菜单栏左上角处，选择服务所在地域：
   - **中国内地**：选择该地域将跳转到**DDoS高防（新BGP）**控制台。
   - **非中国内地**：选择该地域将跳转到**DDoS高防（国际）**控制台。

     您可以通过切换地域分别管理和配置DDoS高防（新BGP）和DDoS高防（国际）实例。在使用DDoS高防服务时，请确认您已选择正确的地域。
3. 在左侧导航栏，选择**接入管理 > 流量调度器**。
4. 在**通用联动**页签，单击**添加规则**。
5. 在**添加规则**面板，配置**阶梯防护**规则，并单击**下一步**。

   DDoS高防（新BGP）阶梯防护规则示例


| 参数 | 描述 |
| --- | --- |
| **联动场景** | 选择**阶梯防护**。 |
| **规则名** | 为规则命名。<br>规则名由英文字母、数字和下划线（_）组成，不超过128个字符。 |
| **高防IP** | 选择要联动的DDoS高防实例。 |
| **联动资源** | 设置要联动的云资源IP：选择云资源所在地域，并输入云资源IP地址。<br>**注意** 云资源IP（ECS、SLB、EIP、WAF）必须已经开启DDoS原生防护企业版防护。相关操作，请参见添加防护对象。<br>单击**添加云资源IP**，可以添加多个云资源。最多支持添加20个IP。<br>**说明** 添加多个云资源IP时（即多个云资源IP关联一个高防IP），如果一个云资源IP上发生DDoS攻击，将优先使用其他云资源IP，直到无可用云资源IP时，才会切换到高防进行防护。如果您希望云产品多路分摊流量，每路被攻击时单独切换高防，请参见多路分摊切换配置。 |
| **回切时间** | 业务流量联动到DDoS高防进行防护后，允许触发回切流程（切换回云资源IP）的等待时间。攻击结束且经过该等待时间后，业务流量自动回切到云资源IP。<br>可选范围：30~120分钟。推荐您设置为60分钟。 |

6. 按照页面提示修改域名的DNS解析设置，并单击**完成**。

   要使联动规则生效，您必须在域名的DNS服务商处修改域名的DNS解析（如果域名通过阿里云域名服务注册，只需在云解析DNS控制台操作；否则需要在注册域名的第三方平台操作），将解析指向流量调度器的CNAME地址。

> **注意** 您修改域名的DNS解析后，流量调度规则将会生效。建议您在修改DNS解析前，先通过修改本地计算机的*hosts*文件配置，验证流量调度规则，避免因回源策略不一致出现不兼容问题。例如，在CDN和高防联动且回源到OSS的场景，由于CDN回源支持修改回源HOST，而DDoS高防不支持，导致发生攻击自动切换到DDoS高防后，DDoS高防回源到OSS的正常流量无法被识别，出现业务故障。

关于验证流量调度规则的操作，请参见本地验证转发配置生效。

关于修改域名DNS解析的操作，请参见修改CNAME解析接入流量调度器。

配置阶梯防护联动规则后，云资源IP的业务流量默认由DDoS原生防护企业版防护；只有在云资源IP上发生大流量DDoS攻击时，业务流量才会自动切换到DDoS高防进行清洗，保证只有正常业务流量会转发到云资源。业务流量自动切换到DDoS高防后，DDoS高防将在攻击结束后等待一段时间（**回切时间**），自动将业务流量回切到云资源（由DDoS原生防护企业版进行防护）。

除了自动切换方式，您还可以选择手动切换，即根据业务防护需求，手动将业务流量切换到DDoS高防、回切到云资源。更多信息，请参见相关操作。

## 相关操作

成功添加通用联动规则后，您可以在规则列表，对已添加的规则执行以下操作。

| 操作 | 说明 |
| --- | --- |
| **切到高防** | 在未自动触发DDoS高防清洗（**联动资源**下有<br>●<br>图标）时，手动将业务流量切换到DDoS高防进行清洗。适用于在业务触发黑洞前提前切换，减少业务损伤。<br>  <br><br>只有当DDoS高防IP不在黑洞中，才可以正常切换到DDoS高防。<br>**注意** 手动将业务流量切换到DDoS高防后，默认不会自动回切到联动资源。如需回切到联动资源，您必须手动执行**回切**操作。 |

| 操作 | 说明 |
| --- | --- |
| **回切** | 在业务流量由DDoS高防清洗（**高防IP**下有<br>●<br>图标）时，手动将业务流量回切到联动资源。<br>  <br><br>**注意**<br>• 建议您在执行回切前，确认攻击已经结束并且回切的联动资源线路可用，避免联动资源处于沙箱状态导致业务中断。<br>• 如果您通过**切到高防**操作将业务流量切换到DDoS高防，则只能通过**回切**操作将流量回切到联动资源。<br>如果联动资源全部在黑洞中，回切操作将会失败。如果有部分联动资源已经解除黑洞，部分联动资源还在黑洞中，流量将先回切到已经解除黑洞的联动资源上，其他资源等待黑洞解除后自动恢复流量。 |
| **编辑** | 编辑通用联动规则，修改除**联动场景**、**规则名**以外的参数配置。 |
| **删除** | 删除通用联动规则。<br>**警告** 删除联动规则前，请确保网站域名的解析没有指向流量调度器CNAME，否则删除联动规则后，网站将无法正常访问。 |

# 4.4.4. CDN/DCDN联动调度

CDN/DCDN联动调度表示通过自定义规则，联动使用DDoS高防与阿里云CDN或DCDN加速服务，实现在业务正常访问期间，流量不经过高防清洗，就近使用CDN或DCDN节点加速；仅在业务被攻击时，流量切换到DDoS高防进行清洗。

## 前提条件

- 已为网站域名开启CDN或DCDN加速。

  相关操作，请参见添加加速域名（CDN联动）、添加加速域名（DCDN联动）。
- 已购买**增强功能**套餐的DDoS高防（新BGP）专业版实例或DDoS高防（国际）保险版、无忧版实例。

  **注意** DDoS高防实例的业务带宽、QPS等规格必须满足正常业务防护需求。

  相关操作，请参见购买DDoS高防实例。
- 已将网站业务接入DDoS高防实例进行防护。

  相关操作，请参见添加网站。
- 已验证DDoS高防实例可以正常转发业务流量。

  相关操作，请参见本地验证转发配置生效。

## 使用限制

使用CDN/DCDN联动需要满足以下限制条件。

| 限制项 | 说明 |
| --- | --- |
| 业务类型 | 只适合HTTP和HTTPS业务，不支持视频直播。 |
| 业务场景 | CDN/DCDN联动不适合以下业务场景：<br>• 被攻击频率太高（例如，高于每周3次以上）的网站。<br>• 对防护生效速度要求比较高的场景。<br>说明 调度到DDoS高防时，防护生效时间受DNS TTL生效时间限制。<br>• 正常业务流量和QPS比较大的场景。<br>说明 如果您的业务超过3 Gbps、10000 QPS，请提交工单进行评估。 |
| CDN或DCDN状态 | CDN或DCDN的加速域名不允许是切入沙箱状态。<br>说明 如果域名已经被CDN或DCDN切入沙箱，建议您只使用DDoS高防，不用联动。 |

## 自动切换的条件

添加CDN/DCDN联动规则时，您需要设置访问QPS阈值，作为CDN/DCDN和DDoS高防间自动相互切换的条件。

自动切换需要满足的具体条件如下：

- CDN/DCDN切换到高防：
  - 连续3分钟内3次触发QPS超过阈值或连续10分钟内出现6次以上，并且CDN/DCDN上流量不超过10 Gbps，触发切换流程。
  - 当高防侧监测到域名进入沙箱状态，并且CDN/DCDN上流量不超过10 Gbps，触发切换流程。
- 高防回切到CDN/DCDN：
  - 连续12小时以上，域名QPS低于QPS阈值的80%、CC阻断率低于10%，触发回切流程。
  - 回切检查：要切回的高防IP不在清洗中、黑洞中和沙箱状态且1小时内不存在清洗、黑洞事件。
  - 回切时间范围：上午08时到晚上23时，其他时间不触发回切。

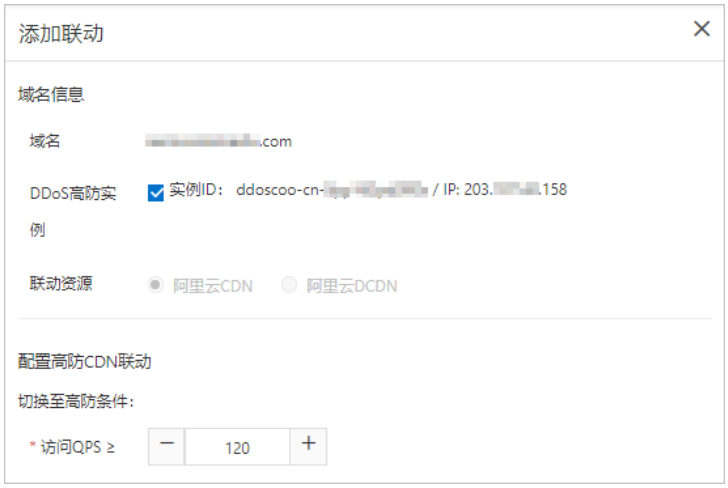
## 添加联动规则

以下操作步骤描述了在DDoS高防控制台配置CDN/DCDN联动DDoS高防的方法，您也可以在CDN控制台配置CDN联动DDoS高防。相关操作，请参见配置CDN联动DDoS高防。

1. 登录DDoS高防控制台。
2. 在顶部菜单栏左上角处，选择服务所在地域：
   - **中国内地**：选择该地域将跳转到**DDoS高防（新BGP）**控制台。
   - **非中国内地**：选择该地域将跳转到**DDoS高防（国际）**控制台。

您可以通过切换地域分别管理和配置DDoS高防（新BGP）和DDoS高防（国际）实例。在使用DDoS高防服务时，请确认您已选择正确的地域。

3. 在左侧导航栏，选择**接入管理 > 流量调度器**。
4. 单击**CDN/DCDN联动调度**页签。
5. 定位到要配置的域名，单击**操作**列下的**添加联动**。
6. 在**添加联动**面板，完成联动配置，并单击**下一步**。




| 参数 | 说明 |
| --- | --- |
| **DDoS高防实例** | 从当前域名已关联的DDoS高防实例中，选择要与CDN/DCDN联动的DDoS高防实例。<br>DDoS高防实例必须是**增强功能**套餐实例。如果提示**该实例需要购买增强功能才可使用CDN联动功能**，请按照页面提示，将实例升级为增强功能套餐再进行设置。<br>如果提示**未选择DDoS高防实例**，请先完成域名接入。相关操作，请参见添加网站。 |
| **联动资源** | 如果当前域名已完成**阿里云CDN**、**阿里云DCDN**配置，则自动选择对应的联动资源，无需手动操作。<br>如果当前域名未完成**阿里云CDN**、**阿里云DCDN**配置，您需要手动选择**阿里云CDN**或**阿里云DCDN**，并按照页面提示前往配置。 |
| **访问QPS** | 设置触发切换到DDoS高防的最小QPS值。关于CDN/DCDN与高防的具体切换条件，请参见自动切换的条件。<br>**说明** 建议您在设置QPS阈值时，考虑业务突增的情形，将阈值设置为业务历史峰值的2~3倍以上，即使网站QPS较低，QPS阈值也建议不要低于500。 |

7. 按照页面提示修改域名的DNS解析设置，并单击**完成**。

要使联动规则生效，您必须在域名的DNS服务商处修改域名的DNS解析（如果域名通过阿里云域名服务注册，只需在云解析DNS控制台操作；否则需要在注册域名的第三方平台操作），将解析指向流量调度器的CNAME地址。

> **注意** 您修改域名的DNS解析后，流量调度规则将会生效。建议您在修改DNS解析前，先通过修改本地计算机的*hosts*文件配置，验证流量调度规则，避免因回源策略不一致出现不兼容问题。例如，在CDN和高防联动且回源到OSS的场景，由于CDN回源支持修改回源HOST，而DDoS高防不支持，导致发生攻击自动切换到DDoS高防后，DDoS高防回源到OSS的正常流量无法被识别，出现业务故障。

关于验证流量调度规则的操作，请参见本地验证转发配置生效。

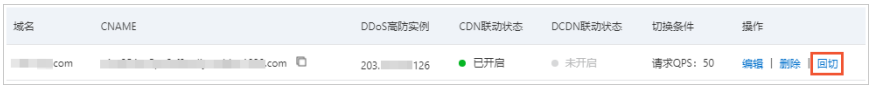
关于修改域名DNS解析的操作，请参见修改CNAME解析接入流量调度器。

配置CDN/DCDN联动调度规则后，如果域名的访问QPS不满足切换到高防的条件，业务流量不经过DDoS高防清洗，就近使用CDN或DCDN节点加速；只有当域名的访问QPS满足切换到高防的条件时，业务流量才会自动切换到DDoS高防进行清洗，保证只有正常业务流量会转发到源站服务器。业务流量自动切换到DDoS高防后，DDoS高防将在满足回切到CDN/DCDN条件时，自动将业务流量回切到CDN/DCDN。

除了自动切换方式，您还可以选择手动切换，即根据业务防护需求，手动将业务流量切换到DDoS高防、回切到CDN/DCDN。更多信息，请参见相关操作。

## 相关操作

成功添加CDN/DCDN联动调度规则后，您可以在规则列表，对已添加的规则执行以下操作。

| 操作 | 说明 |
| --- | --- |
| **切到高防** | 在未自动触发DDoS高防清洗时，手动将业务流量切换到DDoS高防进行清洗。适用于在业务触发黑洞前提前切换，减少业务损伤。<br>  <br><br>只有当DDoS高防IP不在黑洞中，才可以正常切换到DDoS高防。<br>> **注意** 手动将业务流量切换到DDoS高防后，默认不会自动回切到CDN/DCDN。如需回切到CDN/DCDN，您必须手动执行**回切**操作。 |
| **回切** | 在业务流量由DDoS高防清洗时，手动将业务流量回切到CDN/DCDN。<br>  <br><br>> **注意**<br>> - 建议您在执行回切前，确认攻击已经结束并且CDN/DCDN线路可用，避免CDN/DCDN处于沙箱状态导致业务中断。<br>> - 如果您通过**切到高防**操作将业务流量切换到DDoS高防，则只能通过**回切**操作将流量回切到联动资源。 |
| **编辑** | 编辑CDN/DCDN联动调度规则，修改切换到高防条件（即**访问QPS**参数配置）。 |

| 操作 | 说明 |
| --- | --- |
| **删除** | 删除CDN/DCDN联动调度规则。<br>警告 删除联动规则前，请确保网站域名的解析没有指向流量调度器CNAME，否则删除联动规则后，网站将无法正常访问。 |

# 4.4.5. 出海加速

出海加速表示通过自定义规则，联动使用DDoS高防（国际）保险版或无忧版实例与加速线路实例，实现在业务正常访问期间，流量经过加速线路提升访问速度；在业务被攻击时，流量切换到DDoS高防（国际）进行清洗，只有正常业务流量被转发到源站服务器。

## 前提条件

- 已购买DDoS高防（国际）加速线路实例。

  相关操作，请参见购买DDoS高防（国际）加速线路。
- 已购买DDoS高防（国际）保险版或无忧版实例。

  注意 DDoS高防（国际）保险版或无忧版实例的业务带宽、QPS等规格必须满足正常业务防护需求。

  相关操作，请参见购买DDoS高防（国际）保险版或无忧版实例。
- 已将网站业务接入DDoS高防（国际）进行防护，并为业务关联了保险版或无忧版实例、加速线路实例。

  相关操作，请参见添加网站。
- 已验证保险版或无忧版实例、加速线路实例可以正常转发业务流量。

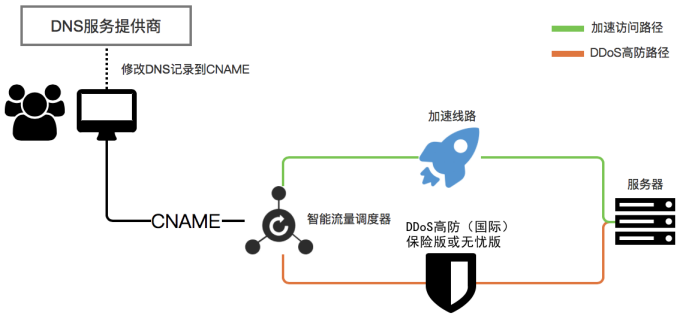
  相关操作，请参见本地验证转发配置生效。

## 背景信息

出海加速联动适用于业务服务器部署在中国内地以外地域，但主要业务用户来自中国内地的场景。该场景下，单独使用DDoS高防（国际）保险版或无忧版实例防护业务，会使中国内地用户访问业务的延时增加。

为避免该影响，您可以同时开通DDoS高防（国际）加速线路，并通过出海加速联动，实现在业务正常访问期间，中国内地用户通过加速线路访问服务器，提升访问速度；仅在业务被攻击时，将业务流量切换到DDoS高防（国际）保险版或无忧版进行清洗。

出海加速联动的实现原理如下图所示。更多信息，请参见配置DDoS高防（国际）加速线路。



## 添加出海加速联动规则

1. 登录DDoS高防控制台。
2. 在顶部菜单栏左上角处，选择**非中国内地**地域。
   选择该地域将跳转到**DDoS高防（国际）**控制台。
3. 在左侧导航栏，选择**接入管理 > 流量调度器**。
4. 在**通用联动**页签，单击**添加规则**。
5. 在**添加规则**面板，配置**出海加速**联动规则，并单击**下一步**。


| 参数 | 说明 |
| --- | --- |
| **联动场景** | 选择**出海加速**。 |
| **规则名** | 为规则命名。<br>规则名由英文字母、数字和下划线（_）组成，不超过128个字符。 |
| **高防IP** | 选择要联动的DDoS高防实例。 |
| **加速线路IP** | 选择要联动的加速线路IP。 |
| **回切时间** | 发生联动后，允许触发回切流程的等待时间。可选项：<br>○ **自动回切**：根据攻击持续时间，自动触发回切。自动回切时间范围：10分钟~60分钟。<br>○ **自定义**：由您设置回切时间。自定义回切时间范围：30分钟~120分钟。为了避免频繁地触发联动切换，建议您设置为60分钟。 |

6. 按照页面提示修改域名的DNS解析设置，并单击**完成**。

   要使联动规则生效，您必须在域名的DNS服务商处修改域名的DNS解析（如果域名通过阿里云域名服务注册，只需在云解析DNS控制台操作；否则需要在注册域名的第三方平台操作），将解析指向流量调度器的CNAME地址。

> **注意** 您修改域名的DNS解析后，流量调度规则将会生效。建议您在修改DNS解析前，先通过修改本地计算机的*hosts*文件配置，验证流量调度规则，避免因回源策略不一致出现不兼容问题。例如，在CDN和高防联动且回源到OSS的场景，由于CDN回源支持修改回源HOST，而DDoS高防不支持，导致发生攻击自动切换到DDoS高防后，DDoS高防回源到OSS的正常流量无法被识别，出现业务故障。

关于验证流量调度规则的操作，请参见本地验证转发配置生效。

关于修改域名DNS解析的操作，请参见修改CNAME解析接入流量调度器。

配置出海加速联动规则后，在业务正常访问期间，中国内地用户通过加速线路访问服务器；在业务被攻击时，业务流量将自动切换到DDoS高防（国际）保险版或无忧版进行清洗，保证只有正常业务流量会被转发到源站服务器。业务流量自动切换到DDoS高防后，DDoS高防将在攻击结束后等待一段时间（**回切时间**），自动将业务流量回切到加速线路。

除了自动切换方式，您还可以选择手动切换，即根据业务防护需求，手动将业务流量切换到DDoS高防（国际）保险版或无忧版、回切到加速线路。更多信息，请参见相关操作。

## 相关操作

成功添加通用联动规则后，您可以在规则列表，对已添加的规则执行以下操作。

| 操作 | 说明 |
| --- | --- |
| **切到高防** | 在未自动触发DDoS高防清洗（**联动资源**下有<br>●<br>图标）时，手动将业务流量切换到DDoS高防进行清洗。适用于在业务触发黑洞前提前切换，减少业务损伤。<br>  <br><br>只有当DDoS高防IP不在黑洞中，才可以正常切换到DDoS高防。<br>**注意** 手动将业务流量切换到DDoS高防后，默认不会自动回切到联动资源。如需回切到联动资源，您必须手动执行**回切**操作。 |

| 操作 | 说明 |
| --- | --- |
| **回切** | 在业务流量由DDoS高防清洗（**高防IP**下有<br>●<br>图标）时，手动将业务流量回切到联动资源。<br>  <br><br>**注意**<br>• 建议您在执行回切前，确认攻击已经结束并且回切的联动资源线路可用，避免联动资源处于沙箱状态导致业务中断。<br>• 如果您通过**切到高防**操作将业务流量切换到DDoS高防，则只能通过**回切**操作将流量回切到联动资源。<br>如果联动资源全部在黑洞中，回切操作将会失败。如果有部分联动资源已经解除黑洞，部分联动资源还在黑洞中，流量将先回切到已经解除黑洞的联动资源上，其他资源等待黑洞解除后自动恢复流量。 |
| **编辑** | 编辑通用联动规则，修改除**联动场景**、**规则名**以外的参数配置。 |
| **删除** | 删除通用联动规则。<br>**警告** 删除联动规则前，请确保网站域名的解析没有指向流量调度器CNAME，否则删除联动规则后，网站将无法正常访问。 |

# 4.4.6. 添加安全加速规则

安全加速适用于业务联动使用DDoS高防（国际）保险版或无忧版实例和安全加速线路，实现以下效果：中国电信和联通以及非移动运营商流量调度到安全加速线路对应的IP上；中国移动和海外流量调度到DDoS高防（国际）对应的IP上。

## 前提条件

- 已开通**DDoS高防（国际）安全加速线路**，并且业务已完成DDoS高防（国际）安全加速线路转发配置。更多信息，请参见购买DDoS高防（国际）安全加速线路和业务接入DDoS高防（国际）安全加速线路。

  **说明** 只需完成业务接入配置，无需修改域名解析。

- 已验证保险版或无忧版实例、加速线路实例可以正常转发业务流量。

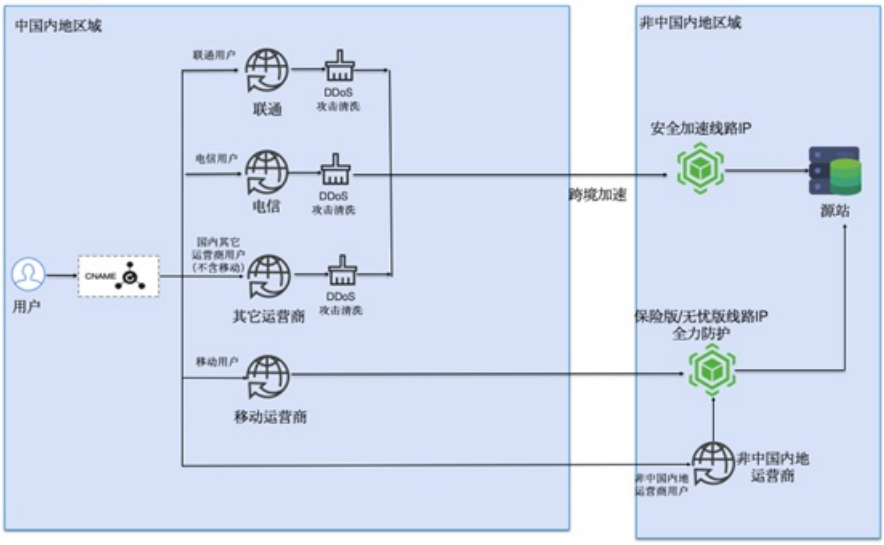
  相关操作，请参见本地验证转发配置生效。

## 背景信息

安全加速线路适用于中国内地地区用户对非中国内地业务加速访问的同时，还可以为中国电信、联通和非移动线路提供大流量DDoS攻击防护能力。

如果您要在保障中国内地地区电信、联通和非移动线路用户的业务访问速度和稳定性的同时，还需要保障中国内地移动运营商和非中国内地运营商用户的业务访问速度和稳定性，可以通过安全加速与DDoS高防（国际）保险版或无忧版结合使用，实现DDoS攻击全力防护。

实现原理如下图所示。




更多信息，请参见配置DDoS高防（国际）安全加速。

## 操作步骤

1. 登录DDoS高防控制台。
2. 在顶部菜单栏左上角处，选择**非中国内地**地域。
   选择该地域将跳转到**DDoS高防（国际）**控制台。
3. 在左侧导航栏，选择**接入管理 > 流量调度器**。
4. 在**通用联动**页签，单击**添加规则**。
5. 在**添加规则**页面，配置**安全加速**规则，并单击**下一步**。

| 参数 | 描述 |
| --- | --- |
| **联动场景** | 选择**安全加速**。 |
| **规则名** | 为规则命名。<br>规则名由英文字母、数字和下划线（_）组成，不超过128个字符。 |
| **安全加速** | 选择要联动的安全加速线路IP。 |
| **国际高防** | 选择要联动的DDoS高防实例。 |

   成功添加规则后，流量调度器为当前规则生成一个CNAME地址。您可以在规则列表中查看已添加的规则和**CNAME**地址。

6. 按照页面提示修改域名的DNS解析设置，并单击**完成**。

   要使联动规则生效，您必须在域名的DNS服务商处修改域名的DNS解析（如果域名通过阿里云域名服务注册，只需在云解析DNS控制台操作；否则需要在注册域名的第三方平台操作），将解析指向流量调度器的CNAME地址。

> 注意　您修改域名的DNS解析后，流量调度规则将会生效。建议您在修改DNS解析前，先通过修改本地计算机的*hosts*文件配置，验证流量调度规则，避免因回源策略不一致出现不兼容问题。例如，在CDN和高防联动且回源到OSS的场景，由于CDN回源支持修改回源HOST，而DDoS高防不支持，导致发生攻击自动切换到DDoS高防后，DDoS高防回源到OSS的正常流量无法被识别，出现业务故障。

关于验证流量调度规则的操作，请参见本地验证转发配置生效。

关于修改域名DNS解析的操作，请参见修改CNAME解析接入流量调度器。

### 相关操作

成功添加通用联动规则后，您可以在规则列表，对已添加的规则执行以下操作。

| 操作 | 说明 |
| --- | --- |
| **编辑** | 编辑通用联动规则，修改除**联动场景**、**规则名**以外的参数配置。 |
| **删除** | 删除通用联动规则。<br>警告　删除联动规则前，请确保网站域名的解析没有指向流量调度器CNAME，否则删除联动规则后，网站将无法正常访问。 |

## 4.4.7. 多路分摊切换配置

本文介绍了在云产品联动和阶梯防护联动场景下需要将多个云资源IP与同一个DDoS高防实例联动时，如何实现云资源多路分摊流量，每路被攻击时单独切换到高防进行防护。

### 云产品联动场景

1. 配置流量调度器。

   为多个云资源IP（例如三个）各自添加一条云产品联动规则，三条规则关联同一个DDoS高防IP。具体操作，请参见云产品联动。

2. 修改域名解析。

   使用同一个主机记录，添加三条CNAME解析记录，记录值分别是步骤1中云产品联动规则的CNAME地址。具体操作，请参见修改CNAME解析接入流量调度器。

3. 验证结果。在DNS检测站点（例如站点之家）上验证步骤2中添加的CNAME记录已经生效。

### 阶梯防护场景

1. 配置DDoS原生防护企业版。

   在DDoS原生防护企业版中添加多个防护对象，例如三个。具体操作，请参见添加防护对象。

2. 配置流量调度器。

   为步骤1中的三个防护对象各添加一条阶梯防护规则，三条规则关联同一个DDoS高防IP。具体操作，请参见阶梯防护。

3. 修改域名解析。

   使用同一个主机记录，添加三条CNAME解析记录，记录值分别是步骤2中三条阶梯防护规则的CNAME地址。具体操作，请参见修改CNAME解析接入流量调度器。

4. 验证结果。在DNS检测站点（例如站点之家）上验证步骤3中添加的CNAME记录已经生效。

# 4.5. 放行DDoS高防回源IP

如果您的源站服务器上部署了非阿里云安全软件（例如防火墙、安全狗等），则您需要在修改DNS解析接入网站业务前，将DDoS高防的回源IP地址加入安全软件的白名单中，避免DDoS高防的回源流量被源站服务器上的安全软件误拦截。

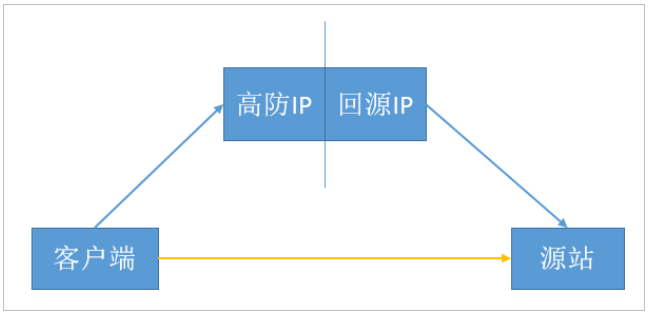
## 前提条件

已在DDoS高防控制台添加网站配置。更多信息，请参见添加网站。

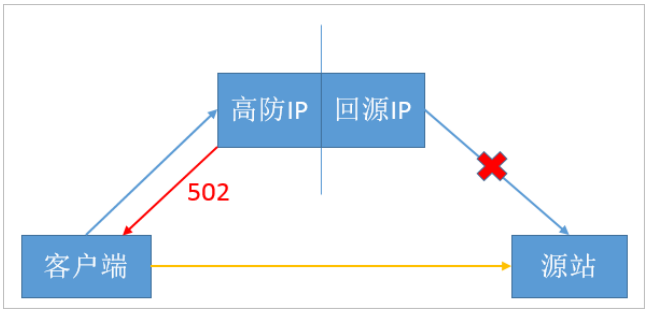
## 背景信息

> **警告** 网站接入DDoS高防进行防护后，网站的正常访问流量将会经过DDoS高防实例清洗，并由DDoS高防回源IP地址转发至源站服务器。因此，如果DDoS高防的回源地址不在源站安全软件的白名单中，访问流量可能被错误拦截，导致网站无法访问。

DDoS高防作为一个反向代理，其中包含了一个Full NAT的架构。没有使用DDoS高防代理时，对于源站来说真实客户端的地址非常分散，且正常情况下每个源IP的请求量都不大。使用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来自高防回源IP段，且分摊到每个回源IP上的请求量会增大很多，这种情况可能会被误认为回源IP在攻击源站。如果源站有其他防御DDoS攻击的安全策略，很可能对回源IP的请求进行拦截或者限速。




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



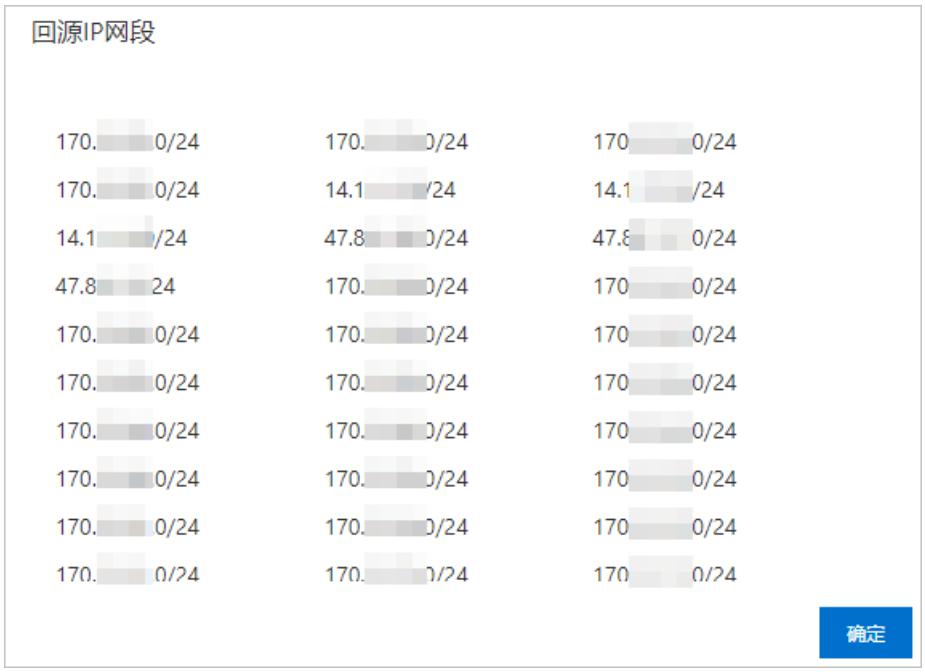

所以，在添加网站配置后，强烈建议您关闭源站上的防火墙和其他安全类软件（例如安全狗等），确保DDoS高防的回源IP不受源站本身安全策略的影响。或者请参见以下操作步骤，在源站服务器的安全软件中设置放行DDoS高防的回源IP地址。

## 操作步骤

1. 登录DDoS高防控制台。

2. 在顶部菜单栏左上角处，选择服务所在地域：
   - **中国内地**：选择该地域将跳转到**DDoS高防（新BGP）**控制台。
   - **非中国内地**：选择该地域将跳转到**DDoS高防（国际）**控制台。

     您可以通过切换地域分别管理和配置DDoS高防（新BGP）和DDoS高防（国际）实例。在使用DDoS高防服务时，请确认您已选择正确的地域。
3. 在左侧导航栏，选择**接入管理 > 域名接入**。
4. 在**域名接入**页面右上方，单击**查看回源IP网段**。
5. 在**回源IP网段**对话框，查看并复制DDoS高防的回源IP网段。




6. 打开源站服务器上的安全软件，将复制的回源IP网段添加到白名单。

# 4.6. 更换源站ECS公网IP

如果您的源站ECS实例的公网IP已不慎暴露，建议您更换ECS实例的公网IP，防止黑客绕过DDoS高防直接攻击源站。您可以在DDoS高防控制台更换ECS实例的公网IP。每个阿里云账号最多可以更换10次。

## 操作步骤

1. 登录DDoS高防控制台。
2. 在顶部菜单栏左上角处，选择服务所在地域：
   - **中国内地**：选择该地域将跳转到**DDoS高防（新BGP）**控制台。
   - **非中国内地**：选择该地域将跳转到**DDoS高防（国际）**控制台。

     您可以通过切换地域分别管理和配置DDoS高防（新BGP）和DDoS高防（国际）实例。在使用DDoS高防服务时，请确认您已选择正确的地域。
3. 在左侧导航栏，选择**接入管理 > 域名接入**。
4. 在**域名接入**页面右上方，单击**更换ECS IP**。
5. 在**更换ECS IP**对话框，单击**知道了，下一步**。

> **注意** 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。


6. （可选）停止ECS实例。

   更换ECS IP需要停止ECS实例。如果您已经停止了需要更换IP的ECS实例，请直接执行下一步。

   如果您还没有停止ECS实例，则可以在**更换ECS IP**对话框，单击**前往ECS**，并在ECS控制台停止需要更换IP的ECS实例。关于停止ECS实例的具体操作，请参见停止实例。


7. 在**更换ECS IP**对话框，输入**ECS实例ID**，并单击**下一步**。
8. 成功释放原IP后，单击**下一步**，为ECS实例自动分配新的IP。
9. ECS IP更换成功后，单击**确认**。

> **说明** 更换IP成功后，请将新的IP隐藏在DDoS高防后面，不要对外暴露。

# 4.7. 配置DDoS高防（国际）加速线路

DDoS高防（国际）加速线路只能与DDoS高防（国际）保险版或无忧版实例结合使用。您将业务（部署在中国内地以外地域）接入DDoS高防（国际）实例防护后，可以通过配置加速线路，实现中国内地用户在无攻击时加速访问受防护的业务。

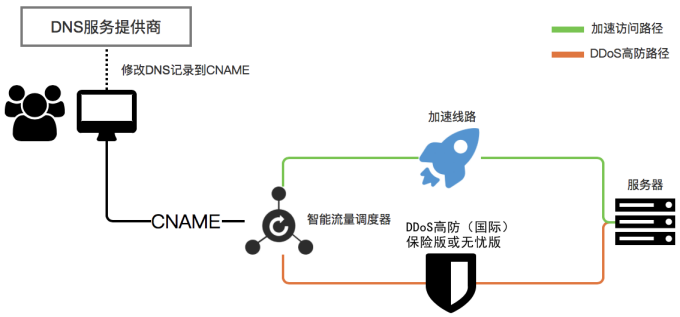
## 前提条件

- 已购买DDoS高防（国际）保险版或无忧版实例。
- 已购买DDoS高防（国际）加速线路。

相关操作，请参见购买DDoS高防实例。

## 背景信息

配置DDoS高防（国际）加速线路，可以在业务在无攻击的情况下，通过加速线路实现业务的快速访问，而当遭受攻击时自动切换到保险版或无忧版实例来缓解DDoS攻击。




## 操作步骤

1. 登录DDoS高防控制台。
2. 在顶部菜单栏左上角处，选择**非中国内地**地域。
   选择该地域将跳转到**DDoS高防（国际）**控制台。
3. 将要防护的业务同时接入DDoS高防（国际）保险版或无忧版实例、加速线路。
   - 网站业务通过**域名接入**方式接入

     您需要在**接入管理 > 域名接入**页面，通过**添加网站**，填写要防护的网站信息。具体操作，请参见添加网站。

     > 注意
     > - 在**填写网站信息**任务中选择**实例**时，必须同时选择保险版或无忧版实例、加速线路。
     > - 只需完成**填写网站信息**任务即可。网站配置成功后，无需按照页面提示修改DNS解析。

   - 非网站业务通过**端口接入**方式接入

     您需要在**接入管理 > 端口接入**页面，通过**添加规则**，配置要防护的业务端口。具体操作，请参见添加规则。

     > 注意
     > - 加速线路只支持接入通过域名指定服务器地址的非网站业务，直接通过IP访问的非网站业务不支持接入加速线路。
     > - 必须分别为保险版或无忧版实例、加速线路配置同样的转发规则。

4. 添加**出海加速**流量调度规则。

   您需要在**接入管理 > 流量调度器**页面的**通用联动**页签，通过**添加规则**，配置**出海加速**规则。具体操作，请参见添加出海加速联动规则。


流量调度规则创建后将生成CNAME，您只需将业务域名的DNS解析指向该CNAME，即可通过流量调度器实现流量的自动调度。

> **注意** 流量自动调度功能基于CNAME，因此域名解析必须使用CNAME方式。

5. 在域名解析服务提供商处，修改业务域名的DNS解析记录。

   要使流量调度规则生效，您必须在域名的DNS服务商处修改域名的DNS解析（如果域名通过阿里云域名服务注册，只需在云解析DNS控制台操作；否则需要在注册域名的第三方平台操作），将解析指向流量调度器的CNAME地址。

   > **注意** 您修改域名的DNS解析后，流量调度规则将会生效。建议您在修改DNS解析前，先通过修改本地计算机的*hosts*文件配置，验证流量调度规则，避免因回源策略不一致出现不兼容问题。

   关于验证流量调度规则的操作，请参见本地验证转发配置生效。

   关于修改域名DNS解析的操作，请参见修改CNAME解析接入流量调度器。

### 执行结果

配置出海加速流量调度规则后，在业务正常访问期间，中国内地用户通过加速线路访问服务器；在业务被攻击时，业务流量将自动切换到DDoS高防（国际）保险版或无忧版实例进行清洗，保证只有正常业务流量会被转发到源站服务器。

# 4.8. 配置DDoS高防（国际）安全加速

DDoS高防（国际）支持安全加速线路，可以实现中国内地地区用户对非中国内地业务加速访问的同时，提供大流量DDoS攻击防护能力。安全加速提供的清洗能力大于2 Tbps，可以有效保障业务访问速度和稳定性。

### 前提条件

您已购买DDoS高防（国际）安全加速线路。更多信息，请参见购买DDoS高防（国际）安全加速线路。

### 背景信息

**安全加速线路**自带DDoS防护清洗能力，在遭受攻击时无需切换至DDoS高防（国际）线路即可缓解DDoS攻击，实现直接进行清洗防护的同时兼顾业务的快速访问。

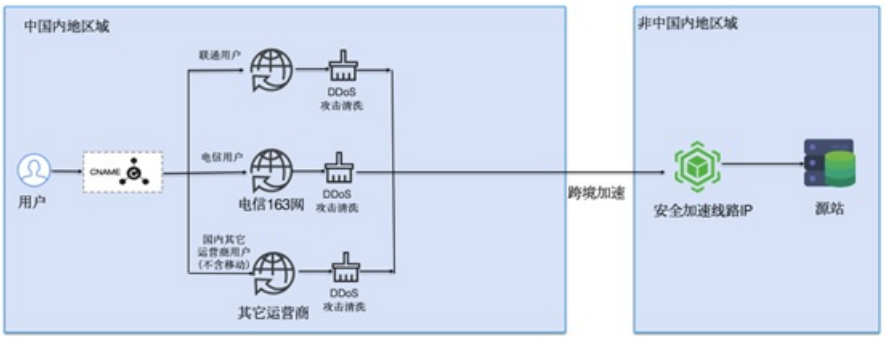
> **说明** **加速线路**由于不带DDoS防护清洗能力，在遭受攻击时只能通过切换至DDoS高防（国际）线路来缓解DDoS攻击。如果攻击频繁，则需频繁切换至DDoS高防（国际）线路。

安全加速线路与出海加速的差异如下。

| 模块 | 功能 | 防护范围 | 攻击切换 | 获得DDoS防护所需的实例规格 |
| --- | --- | --- | --- | --- |
| 安全加速线路 | 加速+DDoS防护（2 T的大流量DDoS攻击清洗） | 防护中国内地地区电信、联通和非移动线路 | 在遭受攻击时，无需通过切换至DDoS高防（国际）线路来缓解DDoS攻击。 | • 防护中国内地地区电信、联通和非移动线路：仅需DDoS高防（国际）安全加速线路<br>• 防护全部运营商线路：需要DDoS高防（国际）保险版或无忧版+安全加速线路 |
| 出海加速 | 仅加速 | 无DDoS防护能力 | 在遭受攻击时，需要通过切换至DDoS高防（国际）线路来缓解DDoS攻击。 | 防护中国内地所有运营商线路：需要DDoS高防（国际）保险版或无忧版+加速线路 |

## 防护中国内地地区电信、联通和非移动线路

如果只需保障中国内地地区电信、联通和非移动线路用户的业务访问速度和稳定性，单独使用DDoS高防（国际）安全加速线路即可。



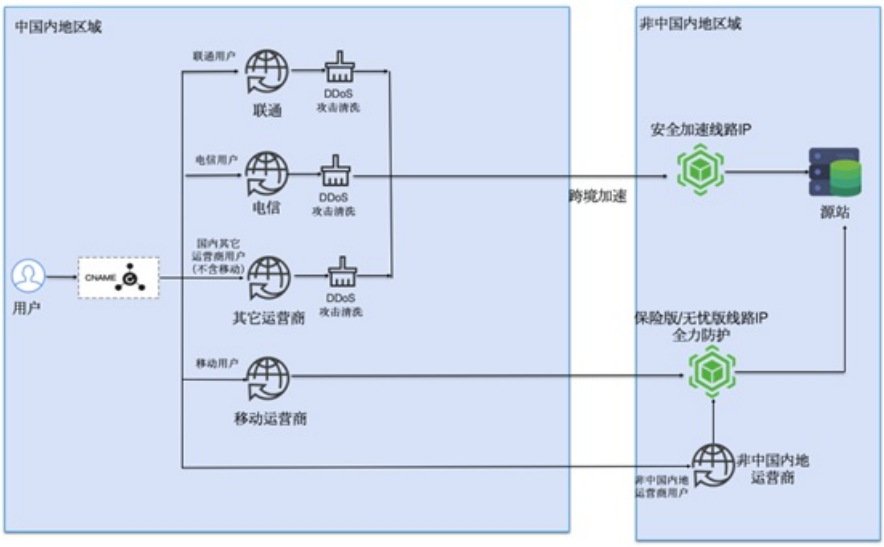

> **说明** 中国内地地区移动用户和海外用户无法直接访问安全加速线路IP，如果需要考虑覆盖，请参见防护全部运营商线路。

1. 登录DDoS高防控制台。
2. 在顶部菜单栏左上角处，选择**非中国内地**地域。
   选择该地域将跳转到**DDoS高防（国际）**控制台。
3. 将您的网站业务或非网站业务配置接入DDoS高防（国际）安全加速线路。
   - 网站域名接入高防（国际）安全加速线路实例：直接选中安全加速线路独享IP。具体接入配置步骤请参见添加网站。
   - 业务端口接入高防（国际）安全加速线路实例：您需要在安全加速线路实例中配置端口转发规则。具体接入配置步骤请参见添加规则。
4. 将业务流量切换到高防（国际）安全加速线路实例，开启安全加速线路对您业务的防护。
   - 网站接入：将您需要防护的网站CNAME解析记录值修改为该网站域名的DDoS高防CNAME地址，详细内容请参见修改DNS解析接入网站业务。

- 端口接入：添加端口规则后，将您需要防护的业务地址设置为高防IP即可。

## 防护全部运营商线路

如果您要在保障中国内地地区电信、联通和非移动线路用户的业务访问速度和稳定性的同时，还需要保障中国内地移动运营商和非中国内地运营商用户的业务访问速度和稳定性，可以通过安全加速与DDoS高防（国际）保险版或无忧版结合使用，实现DDoS攻击全力防护。您需要在**流量调度器**中创建一条安全加速规则。




1. 登录DDoS高防控制台。
2. 在顶部菜单栏左上角处，选择**非中国内地**地域。
   选择该地域将跳转到**DDoS高防（国际）**控制台。
3. 将您的网站业务或非网站业务配置接入DDoS高防（国际）保险版或无忧版安全加速线路实例。

   > **说明** 您只需完成网站或非网站业务接入配置，无需修改DNS解析。

   - 网站域名接入高防（国际）安全加速线路实例：您在选择高防独享IP时，需要同时选择DDoS高防（国际）保险版、无忧版实例和安全加速线路实例的两个独享IP。具体接入配置步骤请参见添加网站。
   - 业务端口接入高防（国际）安全加速线路实例：您需要在DDoS高防（国际）保险版、无忧版实例和安全加速线路实例中配置转发规则，即分别选择DDoS高防（国际）保险版、无忧版实例和安全加速线路实例为您的非网站业务配置转发规则。具体接入配置步骤请参见添加规则。

   > **说明** 业务端口配置接入DDoS高防（国际）安全加速线路仅支持通过域名指定服务器地址的非网站业务。对于业务直接通过IP访问的场景，无法实现业务流量的自动调度。

4. 在**接入管理 > 流量调度器**页面，单击**通用联动**页签。
5. 单击**添加规则**，设置规则条件后，单击**下一步**。
   - **联动场景**：选择**安全加速**。
   - **规则名**：为规则命名。
   - **安全加速**：选择DDoS高防（国际）安全加速实例。
   - **国际高防**：选择DDoS高防（国际）保险版或无忧版实例。

   流量调度规则创建后将生成CNAME，您只需将业务域名的DNS解析指向该CNAME即可通过安全流量调度器实现流量的自动调度：

- 中国内地电信、联通和非移动运营商流量调度到安全加速线路对应的IP上。
- 中国内地移动和海外流量调度到国际高防对应的IP上。

> **说明** 请务必确认调度节点中所选择的独享IP已经完成业务接入配置，可以将流量正常转发回源站服务器。

6. 在域名解析服务提供商处，修改该域名的DNS解析记录。

   将域名解析至安全流量调度规则提供的CNAME，正式将业务流量切换到安全流量调度器，实现自动调度。

> **说明** 流量自动调度功能基于CNAME，因此域名解析必须使用CNAME方式。

# 5.资产管理

## 5.1. 概述

资产管理表示管理DDoS高防服务的资产，具体包括DDoS高防实例、抗D包、全局高级防护。例如，您可以通过资产管理页面购买实例、续费实例、修改实例属性等。本文介绍了DDoS高防（新BGP）、DDoS高防（国际）服务分别支持哪些资产类型及资产管理操作。

### DDoS高防（新BGP）资产管理

下表描述了DDoS高防（新BGP）服务支持的资产类型及资产管理操作。

| 资产类型 | 获取方式 | 说明 | 支持的资产管理操作 |
| --- | --- | --- | --- |
| DDoS高防（新BGP）专业版实例 | 包年包月购买 | 通过中国内地BGP网络，智能防御Tbps级别的DDoS攻击。 | • 购买DDoS高防实例<br>• 修改弹性防护带宽<br>• 升级实例<br>• 续费实例<br>• 管理实例标签 |
| 抗D包 | 不支持购买，特定条件下通过工单申请获得 | 用于抵扣DDoS高防（新BGP）实例触发弹性防护时产生的弹性防护费用。 | DDoS高防抗D包 |

### DDoS高防（国际）资产管理

下表描述了DDoS高防（国际）服务支持的资产类型及资产管理操作。

| 资产类型 | 获取方式 | 说明 | 支持的资产管理操作 |
| --- | --- | --- | --- |
| DDoS高防（国际）保险版、无忧版实例 | 包年包月购买 | 通过全球Anycast网络，近源防御DDoS攻击。 | • 购买DDoS高防实例<br>• 升级实例<br>• 续费实例 |
| 加速线路实例 | 包年包月购买 | 中国内地访问加速组件（无DDoS攻击防御能力），用于提升无攻击情况下的访问质量。<br>**注意** 必须配合DDoS高防（国际）保险版、无忧版实例一起使用。 | |

| 资产类型 | 获取方式 | 说明 | 支持的资产管理操作 |
| --- | --- | --- | --- |
| 安全加速线路实例 | 包年包月购买 | 中国内地访问加速使用，同时具备电信、联通及其他非移动线路的DDoS防御能力。<br>注意 如果需要解决移动线路DDoS防御和非中国内地访问加速，必须配合DDoS高防（国际）保险版、无忧版实例一起使用。 | |
| 全局高级防护 | 按次购买（有效期一年） | 在保险版实例每月提供的2次高级防护耗尽后，增加可用的高级防护次数。<br>注意 必须配合DDoS高防（国际）保险版实例一起使用。 | 购买高级防护资源包 |

# 5.2. 修改弹性防护带宽

购买DDoS高防（新BGP）实例后，您可以根据业务防护需要修改DDoS高防（新BGP）实例的弹性防护带宽。弹性防护带宽决定了DDoS高防（新BGP）实例防御DDoS攻击的最大能力，即该实例能够缓解的DDoS攻击的最大峰值带宽。

## 背景信息

DDoS高防（新BGP）实例具有保底防护带宽、弹性防护带宽，且弹性防护带宽不低于保底防护带宽。由于计费原理不同，保底防护带宽只能通过升级DDoS高防（新BGP）实例进行调整，弹性防护带宽可以随时在DDoS高防（新BGP）控制台修改或者通过升级DDoS高防（新BGP）实例进行调整。

弹性防护带宽越高表示DDoS高防（新BGP）实例能够缓解的DDoS攻击流量的峰值带宽越高。只有当发生了DDoS攻击，且攻击流量的峰值带宽介于保底防护带宽、弹性防护带宽之间时，DDoS高防（新BGP）实例才会在攻击结束后的次日产生本次弹性防护的后付费账单。以下场景下，不会产生弹性防护费用：

- 未发生DDoS攻击，或者发生了DDoS攻击，但是攻击流量不超过保底防护带宽。

  该场景下，依靠保底防护即可防御DDoS攻击。
- 发生了DDoS攻击，但是攻击流量超过了弹性防护带宽。

  该场景下，由于无法防御DDoS攻击，被攻击的资产IP将进入黑洞状态（暂时无法访问），只有等攻击结束后黑洞被解除，业务才会恢复互联网访问。更多信息，请参见 阿里云黑洞策略。

您可以综合考虑业务预计会遭受的DDoS攻击流量的大小、业务防护预算等因素，确定要为DDoS高防（新BGP）实例设置多大的弹性防护带宽。弹性防护带宽最小支持设置为与保底防护带宽一致，表示该实例不使用弹性防护，也不会产生后付费账单。实例的保底防护带宽不同，支持设置的最大弹性防护带宽也不同。例如，保底防护带宽为30 Gbps的实例，最大支持将弹性防护带宽设置为300 Gbps；保底防护带宽大于及等于300 Gbps的实例，最大支持将弹性防护带宽设置为全力防护。

## 前提条件

已购买DDoS高防（新BGP）实例。相关操作，请参见 购买DDoS高防（新BGP）实例。

> **注意** 只有DDoS高防（新BGP）实例有弹性防护带宽属性。DDoS高防（国际）实例默认提供高级防护（即无上限全力防护）能力，无需设置弹性防护带宽。

### 操作步骤

1. 登录DDoS高防控制台。
2. 在顶部菜单栏左上角处，选择**中国内地**地域。
   选择该地域将跳转到**DDoS高防（新BGP）**控制台。
3. 在左侧导航栏，选择**资产管理 > 实例管理**。
4. 定位到要操作的实例，在 **实例状态** 列下，单击 **防护带宽** 后的
   
   图标。
5. 在 **修改弹性带宽** 对话框，为该实例选择一个弹性防护带宽，并单击 **确定** 。
   完成修改后，您可以在 **实例状态** 列下，查看该实例的 **防护带宽** ，其中 **弹性***G** 表示该实例当前的弹性防护带宽为***Gbps。

### 相关问题

DDoS高防（新BGP）弹性计费常见问题

# 5.3. 设置弹性业务带宽

如果您的正常业务流量波动较为频繁或有短期访问突增等特征，建议您为DDoS高防实例启用弹性业务带宽，避免实际业务流量峰值超出实例的业务带宽规格，产生丢包风险。

### 前提条件

已购买DDoS高防（新BGP）实例。

相关操作，请参见购买DDoS高防实例。

### 背景信息

DDoS高防实例默认未启用弹性业务带宽。您将业务接入DDoS高防实例防护后，如果业务的实际流量峰值超出了您在购买实例时选择的**业务带宽**规格（如下图所示），则业务流量转发过程会出现随机丢包现象；业务带宽长期超限，会导致业务被限流，影响业务正常访问。


针对业务带宽超限问题：

- 如果实例的业务带宽规格无法满足正常业务需求，您需要升级实例，提升业务带宽规格。相关操作，请参见升级实例。
- 如果实例的业务带宽规格可以满足日常业务需求，只是无法应对业务流量波动或正常访问量突增的场景，推荐您为DDoS高防实例启用弹性业务带宽。

  通过启用弹性业务带宽，您可以为实例弹性增加带宽承载能力的上限，且只需在实际流量峰值超出业务带宽规格时，为超量使用的业务带宽按使用量支付费用（即弹性业务带宽费用）。关于弹性业务带宽计费方式的详细介绍，请参见弹性业务带宽计费方式。

## 应用场景

如果您接入DDoS高防防护的业务有以下实际业务场景，推荐您为DDoS高防实例启用弹性业务带宽：

- 节假日业务促销：例如，618、双十一等大型促销活动。
- 新业务发布上线：例如，游戏业务开放新服、发布新产品等。
- 网站业务面临窗口期：例如，校园网选课系统、政府网摇号系统等在特定时间段业务访问量突增。

## 使用限制

通过启用弹性业务带宽，DDoS高防（新BGP）实例的业务带宽总和（业务带宽规格加上弹性带宽增加量）最大为5 Gbps，且弹性带宽增加量不超过业务带宽规格的9倍。

示例：

- 假设实例的业务带宽规格为100 Mbps，则带宽最大可以弹性增加900 Mbps。带宽弹性增加后，实例最大可以承载1 Gbps的业务流量。
- 假设实例的业务带宽规格为1 Gbps，则带宽最大可以弹性增加4 Gbps。带宽弹性增加后，实例最大可以承载5 Gbps的业务流量。
- 假设实例的业务带宽规格为5 Gbps，则该实例不支持启用弹性业务带宽。该场景下，如果您需要更高的业务带宽，请提交工单或者联系客户经理。

## 启用弹性业务带宽

1. 登录DDoS高防控制台。
2. 在顶部菜单栏左上角处，选择**中国内地**地域。
   选择该地域将跳转到**DDoS高防（新BGP）**控制台。
3. 在左侧导航栏，选择**资产管理 > 实例管理**。
4. 在实例列表，定位到要操作的实例，在**实例规格**列，单击**带宽弹性增加**后的

   图标。
5. 在**弹性业务带宽**对话框，打开**启用弹性业务带宽**开关，并设置要增加的弹性业务带宽的大小。


弹性业务带宽的最小值为50 Mbps，最大可设置为当前实例业务带宽规格的9倍。例如，如果实例的业务带宽规格为100 Mbps，则弹性业务带宽最大可设置为900 Mbps。

> **注意** 您需要确保增加弹性业务带宽后的业务带宽总和（业务带宽规格加上弹性带宽增加量）不超过5 Gbps，并且大于活动期间正常业务流量的峰值，避免业务流量超限。更多信息，请参见计费示例。

6. 单击**确定**。
   完成以上设置后，您可以在**实例规格**列查看实例的**带宽弹性增加**规格。

启用弹性业务带宽后，如果您需要提升弹性业务带宽，可以参照以上步骤，增加**弹性带宽增加**的值；如果您需要关闭弹性业务带宽，只需关闭**启用弹性业务带宽**开关。

> 注意
> - 针对每个实例，您在一个自然月内只有一次为实例手动关闭弹性业务带宽的机会。如果您在当月关闭了弹性业务带宽，则当月的弹性业务带宽费用根据启用弹性业务带宽期间的实际流量进行结算。
> - 发生以下情况时，弹性业务带宽功能会自动关闭：
>   - 您的DDoS高防实例已过期（实例过期会导致DDoS高防服务不可用）。
>   - 您的阿里云账号发生欠费（账号欠费会导致所有按量计费服务不可用）。
>
> 弹性业务带宽功能自动关闭后，您必须在完成实例续费或者补缴欠费后，手动重新启用弹性业务带宽，才可以继续使用该功能。

您可以在**调查分析 > 操作日志**页面，查看弹性业务带宽的操作记录，例如启用、修改、关闭弹性业务带宽。具体操作，请参见查询操作日志。

## 查询弹性业务带宽账单

启用弹性业务带宽后，您可以在DDoS高防控制台的**调查分析 > 系统日志**页面，查询每个自然月的弹性业务带宽账单。

弹性业务带宽按照自然月出账。出账规则如下：

- 每个自然月的首日上午10时左右，DDoS高防会通过**系统日志**页面，为您推送上个自然月的弹性业务带宽账单（待出账），并通过短信、邮件和站内信的方式，向您的阿里云账号联系人发送推账通知。

  此时账单状态为**待出账**（仍未正式出账），只统计了您在上一个自然月启用弹性业务带宽后产生的弹性带宽用量。您可以通过查看账单详情，了解上个自然月的实际带宽用量。具体操作，请参见查询系统日志。

  如果您对实际带宽用量有疑问，请提交工单咨询。如果经核实，账单出具的用量与您的实际用量有出入，DDoS高防会**终止出账**（即结束该账单，不产生实际费用）。
- 您核实已出具的账单无误后，在该自然月的第10日上午10时，DDoS高防会通过**系统日志**页面，为您推送上个自然月的弹性业务带宽实际出账账单（正式出账）。

  此时账单状态为**已出账**，阿里云将从您的账号余额中扣除实际出账的费用。请保证您的阿里云账号余额充足，避免因账号欠费导致按量计费服务（包含弹性业务带宽）无法使用。

# 5.4. 升级实例

购买DDoS高防实例后，如果实例规格（例如功能套餐、防护域名数、端口数或业务带宽等）无法满足您的实际业务需要，您可以在DDoS高防控制台升级实例规格。本文介绍了升级实例规格的具体操作。

## 前提条件

已购买DDoS高防实例。相关操作，请参见购买DDoS高防实例。

## 背景信息

升级实例表示提升当前DDoS高防实例的规格配置。升级实例需要补齐实例在剩余有效期内对应的规格差价。DDoS高防实例经升级后，不支持降低到原先配置。

> 注意 DDoS高防实例仅支持升级，不支持降配（即降低当前DDoS高防实例的规格配置）。

## 适用的资产类型及可升级规格

升级操作适用于下表描述的DDoS高防资产类型。

| 资产类型 | 支持升级的规格 |
| --- | --- |
| DDoS高防（新BGP）专业版实例 | 保底防护带宽、弹性防护带宽、业务带宽、功能套餐、防护域名数、业务QPS、端口数 |
| DDoS高防（国际）保险版、无忧版实例 | 防护套餐（仅保险版实例支持从保险防护升级到无限防护）、业务带宽、功能套餐、防护域名数、业务QPS、端口数 |
| DDoS高防（国际）加速线路实例 | 业务带宽 |
| DDoS高防（国际）安全加速线路实例 | 业务带宽、功能套餐、防护域名数、业务QPS、端口数 |

## 操作步骤

1. 登录DDoS高防控制台。
2. 在顶部菜单栏左上角处，选择服务所在地域：
   - **中国内地**：选择该地域将跳转到**DDoS高防（新BGP）**控制台。
   - **非中国内地**：选择该地域将跳转到**DDoS高防（国际）**控制台。

     您可以通过切换地域分别管理和配置DDoS高防（新BGP）和DDoS高防（国际）实例。在使用DDoS高防服务时，请确认您已选择正确的地域。
3. 在左侧导航栏，选择**资产管理 > 实例管理**。
4. 定位到要升级的DDoS高防实例，单击**操作**列下的**升级**。
5. 在**变配**页面，根据需要提升当前实例的配置，选中**服务协议**并单击**立即购买**。
6. 完成支付。

完成升级操作后，您可以在**实例管理**页面查看升级后的实例配置。

# 5.5. 续费实例

在DDoS高防实例被释放前，您可以通过手动续费，延长实例的有效期。为了避免因忘记及时续费导致影响业务，您也可以在实例到期前开启自动续费，由阿里云在实例即将到期时自动为实例续费。本文介绍了为实例手动续费、开启自动续费的具体操作。

## 前提条件

已购买DDoS高防实例。相关操作，请参见购买DDoS高防实例。

## 适用的资产类型

续费操作适用于以下DDoS高防资产类型：

- DDoS高防（新BGP）专业版实例
- DDoS高防（国际）保险版、无忧版实例

- DDoS高防（国际）加速线路实例
- DDoS高防（国际）安全加速线路实例

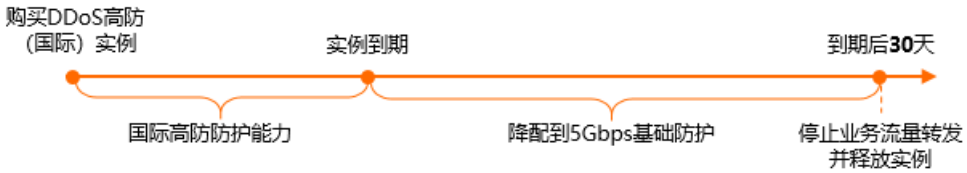
## 实例到期的影响

DDoS高防（新BGP）实例到期后，如果您没有及时为实例续费，会给业务带来以下影响。


| 时间段\到期影响 | 防护能力 | 业务流量转发 | 实例配置 |
| --- | --- | --- | --- |
| 到期时~到期后7个（不含）自然日内 | 失去DDoS高防（新BGP）实例的防护能力，降配到5 Gbps的基础防护能力。<br>此时为实例续费，可以恢复使用DDoS高防（新BGP）实例的防护能力。 | 正常转发业务流量。 | 保留实例配置。 |
| 到期后7个（含）~15个（不含）自然日 | 5 Gbps基础防护能力。 | 停止转发业务流量。<br>警告 如果您暂时不需要继续使用DDoS高防（新BGP）服务，请务必在实例到期7个自然日之前，将业务流量从高防切换到源站服务器（网站业务确保域名解析未指向DDoS高防的CNAME地址、非网站业务确保业务IP未使用高防独享IP），否则将因实例到期影响业务访问。<br>此时为实例续费，可以恢复业务流量转发，无需重新配置实例。 | 保留实例配置。 |

| 时间段\到期影响 | 防护能力 | 业务流量转发 | 实例配置 |
| --- | --- | --- | --- |
| 到期后15个（含）自然日及以后 | 5 Gbps基础防护能力。 | 停止转发业务流量。 | DDoS高防（新BGP）实例将被释放。<br>警告 阿里云账号下的所有DDoS高防（新BGP）实例都已释放后，您在DDoS高防（新BGP）中添加的相关配置（例如域名接入配置、端口接入配置、防护设置、报表数据等）将被永久删除。后续如果您需要再次使用DDoS高防（新BGP）服务，必须重新购买并配置实例。 |

DDoS高防（国际）实例到期后，如果您没有及时为实例续费，会给业务带来以下影响。




| 时间段\到期影响 | 防护能力 | 业务流量转发 | 实例配置 |
| --- | --- | --- | --- |
| 到期时~到期后30个（不含）自然日内 | 失去DDoS高防（国际）实例的防护能力，降配到5 Gbps的基础防护能力。<br>此时为实例续费，可以恢复使用DDoS高防（国际）实例的防护能力。 | 正常转发业务流量。 | 保留实例配置。 |

| 时间段\到期影响 | 防护能力 | 业务流量转发 | 实例配置 |
| --- | --- | --- | --- |
| 到期后30个（含）自然日及以后 | 5 Gbps基础防护能力。 | 停止转发业务流量。<br>警告 如果您暂时不需要继续使用DDoS高防（国际）服务，请务必在实例到期30个自然日之前，将业务流量从高防切换到源站服务器（网站业务确保域名解析未指向DDoS高防的CNAME地址、非网站业务确保业务IP未使用高防独享IP），否则将因实例到期影响业务访问。 | DDoS高防（国际）实例将被释放。<br>警告 阿里云账号下的所有DDoS高防（国际）实例都已释放后，您在DDoS高防（国际）中添加的相关配置（例如域名接入配置、端口接入配置、防护设置、报表数据等）将被永久删除。后续如果您需要再次使用DDoS高防（国际）服务，必须重新购买并配置实例。 |

## 手动续费

在DDoS高防（新BGP）实例、DDoS高防（国际）实例被释放前，您可以为实例手动续费，并继续使用实例的原有配置。

> 注意 如果DDoS高防（新BGP）实例、DDoS高防（国际）实例已经被释放，则不支持手动续费。更多信息，请参见实例到期的影响。

关于手动续费时间的建议如下：

- DDoS高防（新BGP）实例：建议您在实例到期前，最晚不超过实例到期后的7个自然日内，为DDoS高防（新BGP）实例续费，避免影响业务流量转发。
- DDoS高防（国际）实例：建议您在实例到期前，最晚不超过实例到期后的30个自然日内，为DDoS高防（国际）实例续费，避免影响业务流量转发。

参照以下步骤，为DDoS高防（新BGP）实例、DDoS高防（国际）实例手动续费：

1. 登录DDoS高防控制台。
2. 在顶部菜单栏左上角处，选择服务所在地域：
   - **中国内地**：选择该地域将跳转到**DDoS高防（新BGP）**控制台。
   - **非中国内地**：选择该地域将跳转到**DDoS高防（国际）**控制台。

     您可以通过切换地域分别管理和配置DDoS高防（新BGP）和DDoS高防（国际）实例。在使用DDoS高防服务时，请确认您已选择正确的地域。
3. 在左侧导航栏，选择**资产管理 > 实例管理**。
4. 定位到要续费的DDoS高防实例，单击**操作**列下的**续费**。
5. 在**续费**页面，设置**购买时长**（表示续费时长）并选中**服务协议**，单击**立即购买**。


6. 完成支付。

成功续费后，您可以在实例列表中查看实例的**到期时间**，已续费的DDoS高防实例的到期时间将按照您设置的续费时长向后顺延。

## 开启自动续费

自动续费仅支持在实例到期前2个及以上自然日内开启。如果您的实例将于次日到期，请选择手动续费。

参照以下步骤，为DDoS高防（新BGP）实例、DDoS高防（国际）实例开启自动续费：

1. 登录DDoS高防控制台。
2. 在顶部菜单栏，选择**费用 > 续费管理**。


3. 在**手动续费**页签，定位到要续费的DDoS高防（新BGP）、DDoS高防（国际）实例，单击**操作**下的**开通自动续费**。
4. 在**开通自动续费**对话框，选择**自动续费周期**，并单击**开通自动续费**。

成功开通自动续费后，您可以在**自动续费**页签查看实例的自动续费配置。阿里云将于该实例到期前9个自然日，从您的阿里云账号中扣除实例续费所需费用，按照您设置的自动续费周期，延长该实例的有效期。

如果您后续不再需要自动续费，可以在**自动续费**页签为实例执行**恢复手动续费**操作。

# 5.6. 管理实例标签

DDoS高防（新BGP）实例支持通过自定义标签进行分类和检索。您可以自定义标签并标记具有相同用途、属性的DDoS高防实例，实现实例分类和批量检索。本文介绍了为DDoS高防（新BGP）实例创建并绑定标签、移除标签，以及通过标签搜索实例的操作方法。

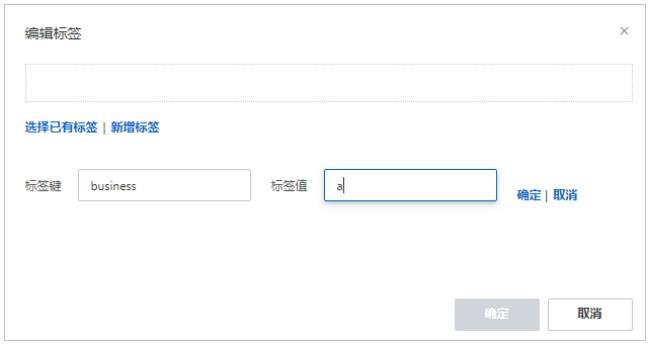
## 背景信息

每个标签都由一对键值对（Key-Value）组成。DDoS高防实例标签有以下使用限制：

- 只有**中国内地**的DDoS高防实例（即新BGP高防实例）支持设置标签。
- 一个实例最多可以绑定20个标签。
- 一个实例上的每个标签的标签键必须唯一，相同标签键的标签值会被覆盖。
- 不支持未绑定实例的空标签存在，即标签必须绑定在某个DDoS高防实例上。

## 添加标签

1. 登录DDoS高防控制台。
2. 在顶部菜单栏左上角处，选择**中国内地**地域。
   选择该地域将跳转到**DDoS高防（新BGP）**控制台。
3. 在左侧导航栏，选择**资产管理 > 实例管理**。
4. 在**实例管理**页面，定位到要操作的实例，单击**实例信息**列**标签**后的
   
   图标。
5. 在**编辑标签**对话框，为实例设置标签。
   支持以下设置方式：
   - 选择已有标签：单击**选择已有标签**，从已有标签列表中选择要使用的标签键和标签值。
   - 新增标签：单击**新增标签**，设置新的**标签键**和**标签值**，并单击**确定**。

   
   
   支持为该实例同时设置多个标签。
6. 单击**确定**。
   成功添加标签后，您可以在**实例信息**中查看已有标签。

## 通过标签搜索实例

1. 登录DDoS高防控制台。
2. 在顶部菜单栏左上角处，选择**中国内地**地域。
   选择该地域将跳转到**DDoS高防（新BGP）**控制台。
3. 在左侧导航栏，选择**资产管理 > 实例管理**。
4. 在**实例管理**页面，从搜索项列表中选择**标签**、标签键和标签值。


符合您选择条件的实例将显示在实例列表。

## 删除标签

DDoS高防不支持批量删除多个实例的标签，您只能单独对某一个实例进行标签删除操作。

1. 登录DDoS高防控制台。
2. 在顶部菜单栏左上角处，选择**中国内地**地域。
   选择该地域将跳转到**DDoS高防（新BGP）**控制台。
3. 在左侧导航栏，选择**资产管理 > 实例管理**。
4. 在**实例管理**页面，定位到要操作的实例，单击**实例信息**列**标签**后的

   图标。
5. 在**编辑标签**对话框，单击要移除的标签的

   图标，并单击**确定**。

> **说明** 当一个标签从一个实例上移除后，如果该标签键没有和其他实例绑定，系统将自动删除该标签。

# 5.7. DDoS高防抗D包

DDoS高防抗D包是面向DDoS高防（新BGP）用户提供的一项增值服务，帮助您减少DDoS攻击峰值大于保底带宽时产生的弹性防护成本。

## 什么是抗D包

一般情况下，针对DDoS攻击峰值大于保底防护带宽，您可以选择使用弹性防护带宽防御攻击或者在业务遭受攻击触发黑洞策略后解除黑洞状态。

- 若使用弹性防护，您根据攻击峰值调整弹性防护值；成功防护后，基于当日成功防护的攻击峰值相对保底防护带宽的超出部分产生后付费（查看弹性防护计费方式）。这种方式带来额外的成本投入。
- 若选择不使用弹性防护（即弹性防护带宽始终等于保底防护带宽），那么当攻击流量超过保底防护带宽时，将触发黑洞；待攻击结束后，使用黑洞解除功能再恢复业务。使用这种方式，您的业务将在一定程度

上受到影响，但不产生额外的弹性后付费成本投入。

DDoS高防抗D包可以在不增加额外成本投入的情况下，帮助您防护超过保底防护带宽的DDoS攻击。

> **说明** 仅DDoS高防（新BGP）支持抗D包。如果您使用DDoS高防（国际），则无法使用抗D包。

抗D包的主要规格参数包括防护规格和可用防护次数。以300 Gbps防护规格，可用防护3次的抗D包为例，具体说明如下：

- 防护规格300 Gbps：表示该抗D包最大可抵扣保底防护带宽+300 Gbps 的攻击峰值所产生的后付费。假如攻击峰值大于保底防护带宽+300 Gbps，那么300 Gbps 抗D包将抵扣失败；抵扣失败时，如果符合DDoS高防后付费产生条件，将会正常产生相应的后付费。
- 可用防护3次：表示该抗D包共可使用3次。无论每日遭受多少次攻击，最多只消耗一次抗D包防护次数。

使用DDoS高防抗D包时，请注意以下内容：

- 抗D包不提升防护能力，仅用于抵扣一次抗D包规格范围内的弹性后付费。您的防护能力仍取决于保底和弹性防护值。

  建议拥有抗D包的高防用户，手动调整弹性防护带宽，以便真正使用上抗D包。您可以将弹性防护带宽最大调整到“保底防护带宽+抗D包规格”。

  例如，保底30 Gbps，抗D包防护规格是300 Gbps，则理论上建议将弹性防护带宽调整为330 Gbps，但仍以实际弹性带宽可调范围为准。


- 只有当攻击峰值-保底防护带宽=<抗D包规格时，才可以通过抗D包成功抵扣弹性后付费。
- 抗D包的可用防护次数消耗到0时，为避免生成不必要的弹性后付费，建议您及时调整弹性防护带宽，使其等于保底防护带宽。
- 抗D包只能抵扣获取该抗D包日期之后产生的后付费（含抗D包获取当天），如果后付费已经产生账单，则无法用抗D包抵扣。

新BGP抗D包和静态高防抗D包的区别

| 对比项目 | 静态高防抗D包 | 新BGP抗D包 |
| --- | --- | --- |
| 使用条件 | 需要绑定具体高防IP才能使用。 | 无需绑定DDoS高防实例。应用时自动匹配剩余有效期最短的抗D包。 |
| 抵扣对象 | 抵扣该抗D包规格范围内攻击峰值的后付费。 | 抵扣攻击峰值减去保底带宽值的超出部分在该抗D包规格范围内的后付费。 |

## 如何获得抗D包

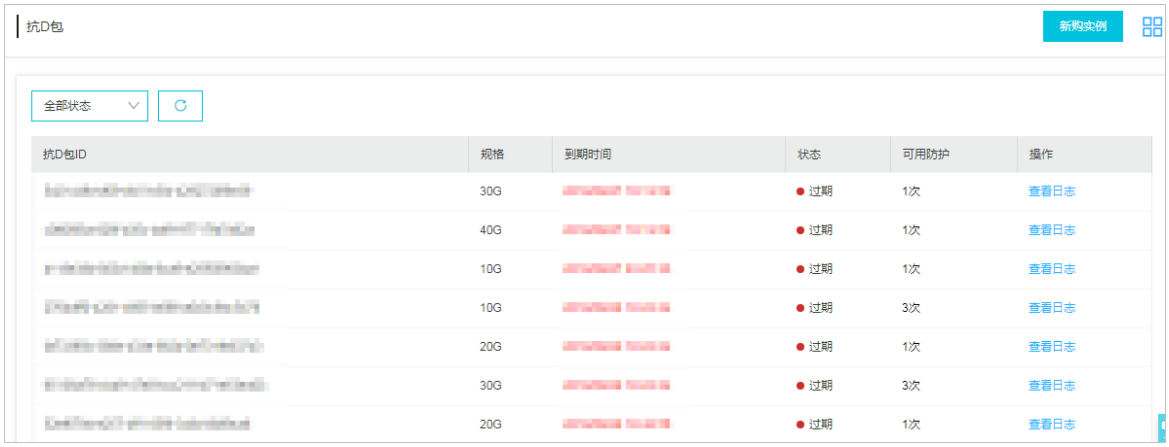
目前，DDoS高防抗D包仅以增值服务的方式向您赠送。如果您符合以下任意一种情况，可以通过客户经理、钉钉服务群或工单向我们申请，免费获得抗D包：

- 首次开通DDoS高防。
- 首次连续使用DDoS高防 3个月以上。
- 包年开通DDoS高防。

## 如何使用抗D包

获得DDoS高防抗D包以后，抗D包会在DDoS攻击触发其防护条件时自动被应用，您可以在DDoS高防控制台查看抗D包详情和消费记录。只有可用防护次数大于0，且未过期的抗D包才是有效的抗D包，可以正常使用。

1. 登录DDoS高防控制台。
2. 在顶部导航栏，选择**中国内地**地域。
3. 在左侧导航栏，选择**资产管理 > 抗D包**。
4. 在**抗D包**页面，查看所有抗D包详情。
   - **抗D包ID**：抗D包的唯一识别标识。
   - **规格**：抗D包的防护规格。
   - **到期时间**：抗D包的有效日期。
   - **状态**：抗D包的状态，分为有效、耗尽和无效。
   - **可用防护**：抗D包的可用防护次数。




5. 单击一个抗D包下的**查看日志**可以查询其操作记录。

# 5.8. 购买高级防护资源包

DDoS高防（国际）保险版实例、安全加速线路实例每月提供两次高级防护。如果实例提供的高级防护无法满足业务防护需求，您可以购买高级防护资源包，扩展实例的防护规格。

## 高级防护资源包适用对象

高级防护资源包分为以下类型：

- 保险版高级防护资源包：只适用于DDoS高防（国际）保险版实例。
- 安全加速线路高级防护资源包：只适用于DDoS高防（国际）安全加速线路实例。

## 高级防护资源包使用方式

保险版实例、安全加速线路实例当月默认高级防护次数消耗完后，如果所防护业务再次遭受大流量攻击（攻击流量超过基础防护阈值），DDoS高防将自动消耗您已购买的高级防护资源包，为业务提供高级防护。

保险版高级防护资源包、安全加速线路高级防护资源包供阿里云账号下所有在有效期内的保险版实例、安全加速线路实例共享使用，无需绑定到具体实例。

高级防护资源包的有效期为1年。您在购买高级防护资源包后，必须在1年内使用资源包，否则资源包过期后将无法使用。

> **注意** 高级防护资源包经购买后，不支持退款。

关于高级防护资源包计费方式的详细介绍，请参见高级防护资源包计费方式。

## 高级防护使用限制

在一个自然月内，阿里云账号下所有DDoS高防（国际）保险版和安全加速线路实例允许使用的高级防护总次数（包括实例默认高级防护和资源包提供的全局高级防护）不能超过20次。否则，高级防护功能将被冻结。

高级防护功能被冻结后，在当前自然月，您将无法继续使用高级防护功能，必须等到下个自然月才能自动恢复使用。

> **说明** 如果您的业务频繁遭受大流量DDoS攻击，建议您选购DDoS高防（国际）无忧版实例（提供不限次数的高级防护）。

## 操作步骤

1. 登录DDoS高防控制台。
2. 在顶部菜单栏左上角处，选择**非中国内地**地域。
   选择该地域将跳转到**DDoS高防（国际）**控制台。
3. 在左侧导航栏，选择**资产管理 > 实例管理**。
4. 在**实例管理**页面右上方，单击**购买**。
5. 在**全局高级防护**购买页面，选择**适用产品**为**保险版**或**安全加速线路**，并选择需要购买的全局高级防护的**次数**。


6. 单击**立即购买**，并完成支付。
   成功购买高级防护资源包后，您可以在实例列表上方查看当前可用的保险版高级防护次数和安全加速线路高级防护次数。


您可以在阿里云用户中心的**资源管理 > 资源包**页面，查看所有已购买的高级防护资源包及资源包的有效期。

# 6.调查分析

## 6.1. 攻击分析

业务流量接入DDoS高防实例进行防护后，您可以通过攻击分析页面查询DDoS高防（新BGP）、DDoS高防（国际）实例上发生的攻击事件记录和详情，了解攻击防护的具体信息，并可以对防护效果进行反馈。本文介绍了使用攻击分析页面的方法。

### 前提条件

- 已购买DDoS高防（新BGP）或DDoS高防（国际）实例。

  相关操作，请参见购买DDoS高防实例。

- 已将业务流量接入DDoS高防（新BGP）或DDoS高防（国际）实例进行防护。

  关于网站类业务接入的具体操作，请参见添加网站。

  关于非网站业务（例如，端游、手游、App等）接入的具体操作，请参见添加规则。

### 背景信息

DDoS高防的**攻击分析**页面向您展示DDoS攻击事件的记录和详情。您可以通过**攻击分析**页面查询历史攻击事件的攻击目标、起止时间、攻击峰值等信息，也可以对攻击防护效果进行反馈。

DDoS攻击事件分为以下类型：

- **流量型**攻击事件：以DDoS高防IP为攻击目标，通常利用大量傀儡机同时发起大量业务请求，通过大流量压垮网络设备和服务器，导致带宽拥塞，服务无法响应。

  如果多个DDoS高防IP在同一时间遭受攻击，则产生多个流量型攻击事件。

- **Web资源耗尽型**攻击事件：以业务域名（已完成域名接入）为攻击目标，通过模拟正常用户请求，频繁访问Web服务中资源消耗较大的页面，大量消耗服务器资源，导致服务器资源耗尽，无法响应正常业务请求。

  如果多个业务域名在同一时间遭受攻击，则产生多个Web资源耗尽型攻击事件。

- **连接型**攻击事件：以业务端口（已完成端口接入）为攻击目标，通过非法占用服务器的TCP、UDP连接通道，大量消耗服务器连接数资源，使服务器无法处理新的连接请求，导致正常业务无法运行。

  如果一个DDoS高防IP下的多个业务端口在同一时间遭受攻击，则产生多个连接型攻击事件。

**攻击分析**页面还支持查看攻击事件详情，帮助您了解攻击来源IP、攻击类型分布、攻击来源地区分布等信息，实现攻击防护流程的透明化，提升防护分析体验。

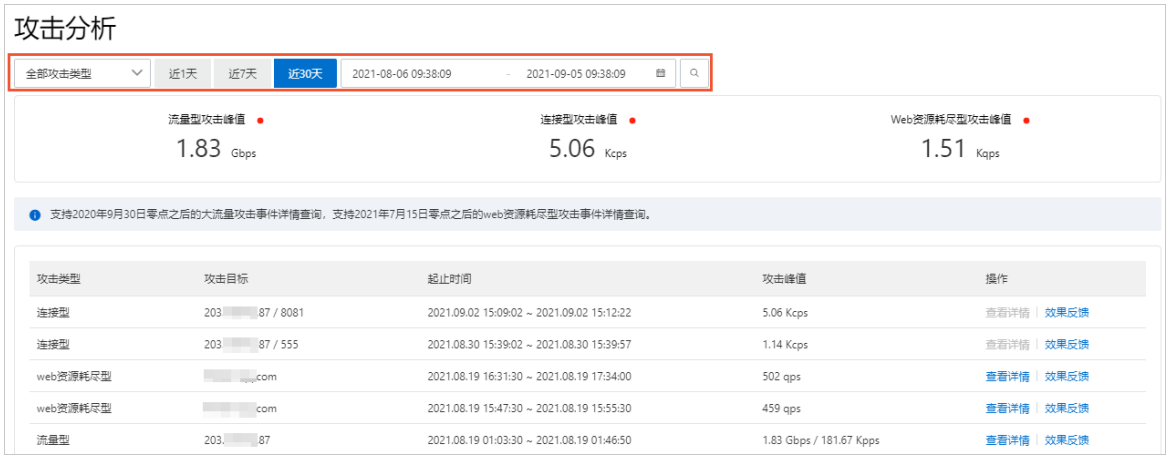
### 查询攻击事件记录

1. 登录DDoS高防控制台。
2. 在顶部菜单栏左上角处，选择服务所在地域：
   - **中国内地**：选择该地域将跳转到**DDoS高防（新BGP）**控制台。
   - **非中国内地**：选择该地域将跳转到**DDoS高防（国际）**控制台。

     您可以通过切换地域分别管理和配置DDoS高防（新BGP）和DDoS高防（国际）实例。在使用DDoS高防服务时，请确认您已选择正确的地域。
3. 在左侧导航栏，选择**调查分析 > 攻击分析**。
4. 在**攻击分析**页面，选择要查询的攻击类型和时间范围，查询相关的攻击记录。

支持的查询条件包括：

- 攻击类型：支持选择**Web资源耗尽型**、**连接型**、**流量型**或**全部攻击类型**。
- 时间范围：支持快速查询**近1天**、**近7天**或**近30天**的攻击事件，也可以自定义查询时间范围。自定义查询时间范围时，最多允许查询最近180天内的攻击事件。




**攻击分析**页面向您展示以下信息：

- 页面上方展示了查询时间范围内的**流量型攻击峰值**（单位：bps）、**连接型攻击峰值**（单位：cps）和**Web资源耗尽型攻击峰值**（单位：qps）。
- 页面下方展示了攻击事件记录。每条攻击事件记录包含**攻击类型**、**攻击目标**、**起止时间**和**攻击峰值**信息。

如果您对某个攻击事件的防护效果有任何建议或疑问，可以通过单击事件**操作**列下的**效果反馈**，向我们反馈。我们会根据您的宝贵意见持续优化和改进防护效果。

DDoS攻击事件支持查看攻击事件详情。您可以单击事件**操作**列下的**查看详情**，查看攻击事件详情。更多信息，请参见查看流量型攻击详情、查看Web资源耗尽型攻击详情、查看连接型攻击详情。

## 查看流量型攻击详情

您可以在**攻击分析**页面，单击某个**流量型**DDoS攻击事件后的**查看详情**，前往**事件详情**页面（如下图所示），查看事件详情并执行相关操作。

> **注意** 只有在2020年09月30日零点以后发生的流量型攻击事件，支持查询事件详情。


**事件详情**页面包含以下内容：

- 页面上方展示了**攻击时间**、**攻击目标**（DDoS高防实例的IP）、**攻击带宽峰值**（单位：bps）和**攻击报文峰值**（单位：pps）信息。

  您可以单击**攻击目标**后的**防护设置**，前往**基础设施DDoS防护**页签，为被攻击实例配置防护策略。相关操作，请参见基础设施DDoS防护。

- **攻击防护详情**：展示了攻击期间，入方向、出方向流量和清洗流量的带宽的变化趋势图（位于**bps**页签）、报文的变化趋势图（位于**pps**页签）。
- **来源IP（Top 10）**：展示了发起请求次数最多的前10个IP及IP所属地区。单击**更多**可以查看Top 100来源IP的信息。

  > **说明** 来源IP包含攻击IP和正常请求IP。

  如果您需要封禁某个IP的流量，可以单击列表下的**黑名单设置**，前往**基础设施DDoS防护**页签，为被攻击实例配置**黑 / 白名单（针对高防实例IP）**防护策略。相关操作，请参见设置黑白名单（针对高防实例IP）。

- **攻击来源运营商**：展示了攻击流量的来源运营商分布。单击**更多**可以查看不同运营商的请求占比数据。

  > **注意** 目前只有DDoS高防（新BGP）支持该数据，DDoS高防（国际）暂不支持该数据。

- **攻击来源地区**：展示了攻击流量的来源地区分布。单击**更多**可以查看不同来源地区的请求占比数据。

  如果您需要封禁某个攻击来源地区的流量，可以单击图表下的**区域封禁设置**，前往**基础设施DDoS防护**页签，为被攻击实例配置**区域封禁**防护策略。相关操作，请参见设置区域封禁。

- **攻击类型**：展示了攻击流量的协议类型分布。单击**更多**可以查看不同攻击类型的请求占比数据。

您可以在**事件详情**页面的右上角，单击**导出报表**，并选择**导出图片**、**导出pdf**，将当前事件详情页面另存为本地文件（PNG格式、PDF格式）。


## 查看Web资源耗尽型攻击详情

您可以在**攻击分析**页面，单击某个**Web资源耗尽型**DDoS攻击事件后的**查看详情**，前往**事件详情**页面（如下图所示），查看事件详情并执行相关操作。

> **注意** 只有在2021年07月15日零点以后发生的Web资源耗尽型攻击事件，支持查询事件详情。


**事件详情**页面包含以下内容：

- 页面上方展示了**攻击时间**、**攻击目标**（域名）、**请求数峰值**（单位：qps）和**总接收请求数**（单位：次）、**总拦截请求数**（单位：次）信息。

您可以单击**攻击目标**后的**防护设置**，前往**网站业务DDoS防护策略**页签，为被攻击域名配置防护策略。相关操作，请参见网站业务DDoS防护。

- **攻击防护详情**：展示了攻击期间，入方向总QPS和触发不同模块下防护策略的QPS的变化趋势图，以及触发的防护策略的**策略生效时间**和**拦截次数**信息。

  网站业务防护模块包括**黑名单**、**区域封禁**、**频率控制**、**精确访问控制**、**其他**（例如人机校验失败等）。关于不同防护模块的配置方法，请参见网站业务DDoS防护。

  您可以在该区域的右上角，设置要查询的时间范围。

- **来源地区**：展示了攻击请求的来源地区分布，支持切换查看**全球**分布（国家维度）、**中国内地**分布（省市区维度）。单击**更多**可以查看不同来源地区的请求占比数据。

  如果您需要封禁某个攻击来源地区的流量，可以单击图表下的**防护设置**，前往**网站业务防护策略**页签，为被攻击域名配置**区域封禁（针对域名）**防护策略。相关操作，请参见设置区域封禁（针对域名）。

- **URL**：展示了被请求次数最多的前5条URL。按照被请求次数由高到低排序。单击**更多**可以查看所有被请求的URL（即URI和所属域名）及不同URL的占比。

  如果您需要针对具体URI配置访问限速策略，可以单击图表下的**防护设置**，前往**网站业务防护策略**页签，为被攻击域名配置**频率控制**防护策略。相关操作，请参见设置频率控制。

- **防护模块过滤分布**：展示了不同防护模块拦截的攻击请求的数量分布。

  您可以单击图表下的**防护设置**，前往**网站业务防护策略**页签，为不同防护模块配置防护策略。关于不同防护模块的配置方法，请参见网站业务DDoS防护。

- **Top10攻防策略**：展示了被命中次数最多的前10条防护策略及其占比。单击**更多**可以查看Top 100攻防策略及不同策略的占比。

  您可以单击图表下的**防护设置**，前往**网站业务防护策略**页签，为不同防护模块配置防护策略。关于不同防护模块的配置方法，请参见网站业务DDoS防护。

您可以在**事件详情**页面的右上角，单击**导出报表**，并选择**导出图片**、**导出pdf**，将当前事件详情页面另存为本地文件（PNG格式、PDF格式）。


## 查看连接型攻击详情

您可以在**攻击分析**页面，单击某个**连接型**DDoS攻击事件后的**查看详情**，前往**事件详情**页面（如下图所示），查看事件详情并执行相关操作。

> **注意** 只有在2021年09月20日零点以后发生的连接型攻击事件，支持查询事件详情。


**事件详情**页面包含以下内容：

- 页面上方展示了**攻击时间**、**攻击目标**（DDoS高防实例的IP及端口）、**并发连接峰值**（单位：conns，表示并发连接次数）和**新建连接峰值**（单位：cps，表示每秒新建连接次数）信息。

  您可以单击**攻击目标**后的**防护设置**，前往**基础设施DDoS防护策略**页签，为被攻击实例配置防护策略。相关操作，请参见基础设施DDoS防护。

- **攻击防护详情**：展示了攻击期间，**新建连接数**和**并发连接数**的变化趋势图。

  新建连接数趋势图包含不同防护策略拦截的异常连接数据，例如，**黑名单**策略、**区域封禁**策略、**源限速**策略（具体分为**源并发连接限速**、**源PPS限速**、**源带宽限速**）。关于以上防护策略的配置方法，请参见设置黑白名单（针对高防实例IP）、设置区域封禁、设置源限速。

  并发连接数趋势图包含**活跃**连接数和**非活跃**连接数的数据。

  您可以在该区域的右上角，设置要查询的时间范围。

- **攻击来源IP**：展示了发起异常连接次数最多的前5个IP及IP所属地区。单击**更多**可以查看Top 100攻击来源IP的信息。

> **说明** 攻击来源IP全部为攻击IP，不包含正常请求IP。

如果您需要封禁某个IP的流量，可以为被攻击实例配置**黑 / 白名单（针对高防实例IP）**防护策略。相关操作，请参见设置黑白名单（针对高防实例IP）。

- **攻击类型**：展示了攻击流量的协议类型分布。单击**更多**可以查看不同攻击类型的请求占比数据。
- **攻击来源地区**：展示了攻击请求的来源地区分布。单击**更多**可以查看不同来源地区的请求占比数据。

  如果您需要封禁某个攻击来源地区的流量，可以为被攻击实例配置**区域封禁**防护策略。相关操作，请参见设置区域封禁。

您可以在**事件详情**页面的右上角，单击**导出报表**，并选择**导出图片**、**导出pdf**，将当前事件详情页面另存为本地文件（PNG格式、PDF格式）。


# 6.2. 全量日志分析

## 6.2.1. 概述

DDoS高防的网站访问日志与阿里云日志服务联动，为您提供全量日志分析服务。全量日志分析是增值服务，需要开通后才可使用。开通全量日志分析后，日志服务将实时采集接入DDoS高防防护的网站业务的日志，并基于采集到的日志数据向您提供日志查询与分析和日志报表服务。

### 什么是全量日志分析

DDoS高防全量日志分析基于阿里云日志服务，在DDoS高防控制台为您提供日志查询与分析页面，方便您对接入DDoS高防的网站业务进行自主分析。开通全量日志后，您也可以使用日志服务提供的日志消费和投递等功能，全面管理DDoS高防的网站访问日志。

关于阿里云日志服务的详细介绍，请参见什么是日志服务。

### 应用场景

DDoS高防全量日志分析服务可以满足您的以下需求：

- 排查网站访问异常

  为网站业务开启日志采集后，您可以对采集到的日志进行实时查询与分析。例如，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。

- 追踪CC攻击者来源

  DDoS高防的网站访问日志中记录了CC攻击者的分布及来源。通过对网站访问日志进行实时查询与分析，您可以追踪CC攻击者的来源、溯源攻击事件，为您的应对策略提供参考。例如，您可以分析CC攻击者的国家分布、查询访问PV等。

- 网站运营分析

  网站访问日志中实时记录了网站访问数据，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。

### 计费信息

全量日志分析服务仅支持以包年包月方式开通。具体价格信息，请参见全量日志服务购买页的价格计算结果。

### 相关文档

| 文档链接 | 说明 |
| --- | --- |
| 快速上手 | 介绍了开通和快速使用全量日志分析的操作方法。<br>注意 首次使用全量日志分析时，您必须参照本文档开通服务并完成服务相关配置。 |
| 全量日志字段说明 | 介绍了DDoS高防日志数据包含的字段。 |
| 查询和分析全量日志 | 介绍了如何通过查询分析语句，对DDoS高防日志数据进行查询与分析。 |
| 查询日志报表 | 介绍了如何使用全量日志分析为您预设的仪表盘图形报表（包括DDoS运营中心、DDoS访问中心）。 |

# 6.2.2. 计费方式

DDoS高防全量日志服务按照包年包月方式计费，根据您已购买的日志存储容量来收取费用。

### 概述

全量日志服务是DDoS高防提供的一项增值服务，采用与DDoS高防实例独立的计费方式。您将网站接入DDoS高防实例防护后，DDoS高防默认不会记录网站的访问日志。如果您需要相关日志数据进行业务分析，必须开通全量日志服务。

全量日志服务按照包年包月方式计费。您可以在全量日志服务购买页，为DDoS高防（新BGP）、DDoS高防（国际）开通全量日志服务。全量日志服务根据您选择的**日志存储量**和**购买时长**计算费用。关于开通全量日志服务的具体操作，请参见步骤1：开通全量日志分析。

开通全量日志服务后，您将获得一个全量日志服务实例。您可以在全量日志服务实例的有效期内，使用全量日志服务采集网站访问日志，并基于采集到的日志数据进行查询与分析、告警配置等。

注意 全量日志服务实例与DDoS高防实例相互独立，需要分开管理。例如，您需要分别为DDoS高防实例、全量日志服务实例续费等。

### 日志存储规格

| 规格名称 | 是否影响计费 | 说明 | 开通全量日志服务后，是否支持修改 |
| --- | --- | --- | --- |

| 规格名称 | 是否影响计费 | 说明 | 开通全量日志服务后，是否支持修改 |
| --- | --- | --- | --- |
| 日志存储容量 | 是 | 开通全量日志服务时，您需要选择日志存储容量（单位：TB）。不同存储容量的具体价格，以全量日志服务购买页为准。 | 支持。<br>开通全量日志服务后，您可以通过以下操作，修改日志存储容量：<br>• 通过升级，提升日志存储容量。具体操作，请参见升级日志存储容量。<br>• 通过降配，降低日志存储容量。具体操作，请参见降配日志存储容量。<br>警告 如果日志存储容量已占满，新的日志数据将无法存储，会导致日志数据丢失。已存储的日志数据将保留，直到该日志数据因超出日志存储时长被自动删除。<br>日志存储容量占满时，您可以选择升级日志存储容量或者清空日志数据。关于清空日志数据的具体操作，请参见清空日志。 |
| 日志存储时长 | 否 | 默认为180天，即只存储最近180天内的日志数据。 | 支持。<br>开通全量日志服务后，您可以在30~180天范围内自定义日志存储时长。具体操作，请参见修改日志存储时长。 |
| 存储对象 | 否 | 只存储已开启日志采集的网站域名的全量日志。 | 支持。<br>开通全量日志服务后，您可以为已接入DDoS高防防护的域名开启或关闭日志采集。具体操作，请参见步骤2：开启日志采集。 |
| 日志字段 | 否 | 关于DDoS高防（新BGP）和DDoS高防（国际）全量日志包含的所有日志字段，请参见全量日志字段说明。 | 不支持。 |

## 如何选择日志存储容量？

您可以参考以下信息，根据网站的日常QPS评估需要的日志存储容量：

每条请求日志大约占用2 KB存储空间，如果网站的平均请求量为500 QPS，则存储一天的日志需要的存储空间为500*60*60*24*2 = 86,400,000 KB（约82 GB）；存储180天的日志需要的存储空间为86,400,000 * 180 = 15,552,000,000 KB（约14.5 TB）。

## 服务到期说明

全量日志服务到期时，会有以下影响：

- DDoS高防将停止存储新的日志数据。
- 已存储的日志数据将为您保留7天。

如果您在服务到期7天内完成续费，则可以继续使用全量日志服务；如果您未能及时完成续费，则已存储的日志数据将被自动清空。

关于全量日志服务续费的具体操作，请参见续费全量日志服务。

# 6.2.3. 全量日志字段说明

本文介绍了DDoS高防全量日志包含的日志字段。

| 字段 | 说明 | 示例 |
| --- | --- | --- |
| __topic__ | 日志主题，取值固定为ddos_access_log，表示DDoS高防日志。 | ddos_access_log |
| body_bytes_sent | 请求发送Body的大小，单位为字节。 | 2 |
| content_type | 内容类型。 | application/x-www-form-urlencoded |
| host | 源网站。 | api.aliyundoc.com |
| http_cookie | 请求Cookie。 | k1=v1;k2=v2 |
| http_referer | 请求Referer。如果没有Referer，返回 - 。 | http://aliyundoc.com |
| http_user_agent | 请求UserAgent。 | Dalvik/2.1.0 (Linux; U; Android 10; Android SDK built for x86 Build/QSR1.200715.002) |
| http_x_forwarded_for | 通过代理跳转的上游用户IP。 | 192.0.XX.XX |
| https | 该请求是否为HTTPS请求。取值：true、false。 | true |
| matched_host | 匹配的配置的源站域名（可能是泛域名）。未匹配到时返回 - 。 | *.aliyundoc.com |
| real_client_ip | 请求的真实来源IP。获取不到时返回 - 。 | 192.0.XX.XX |
| isp_line | 线路信息，例如BGP、电信、联通等。 | 电信 |
| remote_addr | 请求连接的客户端IP。 | 192.0.XX.XX |
| remote_port | 请求连接的客户端端口号。 | 23713 |
| request_length | 请求长度，单位为字节。 | 123 |
| request_method | 请求的HTTP方法。 | GET |
| request_time_msec | 请求时间，单位为毫秒。 | 44 |

| 字段 | 说明 | 示例 |
| --- | --- | --- |
| request_uri | 请求路径。 | /answers/377971214/banner |
| server_name | 匹配到的主机名。如果没有匹配到，返回 `default` 。 | api.aliyundoc.com |
| status | HTTP状态。 | 200 |
| time | 请求时间。 | 2018-05-02T16:03:59+08:00 |
| cc_action | CC防护策略的动作，例如none、challenge、pass、close、captcha、wait、login等。 | close |
| cc_blocks | 请求是否被CC防护策略阻断。取值：<br>• `1` ：表示阻断。<br>• 其他内容表示通过。<br>**说明** 部分情况下，日志中可能不存在该字段。而是以 `last_result` 字段记录请求是否被CC防护策略阻断。 | 1 |
| last_result | 请求对应的最终防护动作。取值：<br>• `ok` ：表示通过。<br>• `failed` ：表示不通过，包括校验未通过和阻断。<br>**说明** 部分情况下，日志中可能不存在该字段。而是以 `cc_blocks` 字段记录请求是否被CC防护策略阻断。 | failed |
| cc_phase | CC防护策略，包括seccookie、server_ip_blacklist、static_whitelist、 server_header_blacklist、server_cookie_blacklist、server_args_blacklist、qps_overmax等。 | server_ip_blacklist |
| ua_browser | 浏览器标识。<br>**说明** 部分情况下，日志中可能不存在该字段。 | ie9 |
| ua_browser_family | 浏览器系列。<br>**说明** 部分情况下，日志中可能不存在该字段。 | internet explorer |

| 字段 | 说明 | 示例 |
| --- | --- | --- |
| ua_browser_type | 浏览器类型。<br>说明 部分情况下，日志中可能不存在该字段。 | web_browser |
| ua_browser_version | 浏览器版本。<br>说明 部分情况下，日志中可能不存在该字段。 | 9.0 |
| ua_device_type | 客户端设备类型。<br>说明 部分情况下，日志中可能不存在该字段。 | computer |
| ua_os | 客户端操作系统标识。<br>说明 部分情况下，日志中可能不存在该字段。 | windows_7 |
| ua_os_family | 客户端操作系统系列。<br>说明 部分情况下，日志中可能不存在该字段。 | windows |
| upstream_addr | 回源地址列表，格式为 `IP:Port` ，多个地址用半角逗号（,）分隔。 | 192.0.XX.XX:443 |
| upstream_ip | 回源IP。 | 192.0.XX.XX |
| upstream_response_time | 回源响应时间，单位为秒。 | 0.044 |
| upstream_status | 回源请求HTTP状态。 | 200 |
| user_id | 阿里云账号ID。 | 166688437215**** |
| querystring | 请求字符串。 | token=bbcd&abc=123 |

# 6.2.4. 快速上手

本文介绍了如何开通和快速使用DDoS高防全量日志分析服务。

## 前提条件

- 已购买DDoS高防实例并将网站业务接入DDoS高防进行防护。相关操作，请参见添加网站。

只有完成网站接入后，您才可以通过全量日志分析采集和存储网站的日志数据，并对采集到的日志数据进行查询与分析。

- 已开通阿里云日志服务。

  首次登录日志服务控制台时，您可以根据页面提示开通日志服务。

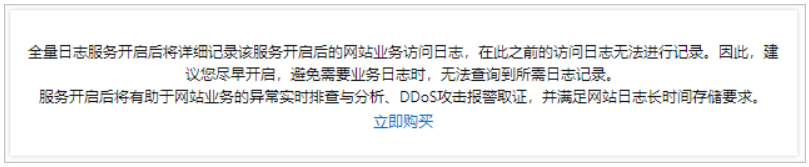
## 步骤1：开通全量日志分析

参照以下步骤，开通DDoS高防全量日志分析服务：

1. 登录DDoS高防控制台。
2. 在顶部菜单栏左上角处，选择服务所在地域：
   - **中国内地**：选择该地域将跳转到**DDoS高防（新BGP）**控制台。
   - **非中国内地**：选择该地域将跳转到**DDoS高防（国际）**控制台。

     您可以通过切换地域分别管理和配置DDoS高防（新BGP）和DDoS高防（国际）实例。在使用DDoS高防服务时，请确认您已选择正确的地域。
3. 在左侧导航栏，选择**调查分析 > 全量日志分析**。
4. 在**全量日志分析**页面，单击**立即购买**。

   如果您已经开通全量日志分析服务，则不会出现**立即购买**按钮，您可以直接使用该服务。相关操作，请参见步骤2：开启日志采集。




5. 在**全量日志**购买页面，完成以下购买配置。


| 参数 | 说明 |
| --- | --- |
| **适用产品** | 选择**新BGP高防**、**DDoS高防（国际）**。 |

| 参数 | 说明 |
| --- | --- |
| **日志存储量** | 选择日志数据的最大存储空间，单位：TB。可选项：3 T、5 T、10 T、20 T、50 T、100 T、1000 T。<br>当日志存储空间足够大且在服务有效期内，将从使用服务的第一天开始，连续存储180天的日志数据。第181天的日志数据，将覆盖第一天存储的日志数据，即始终保持存储最近180天的全量日志数据。<br>一般情况下，每条请求日志大约占用2 KB存储空间，如果您的业务的平均请求量为500 QPS，则一天的日志存储所需要的存储空间为：500*60*60*24*2 = 86,400,000 KB（约82 GB）；系统默认的存储周期为180天，如果您需要存储最近180天的日志，则需要选择的日志存储量规格为14,832 GB（约14.5 TB）。<br>**注意** 当您选购的日志存储空间占满后，将不再继续存储新的日志数据。 |
| **购买时长** | 选择服务有效期。可选项：1个月、2个月、3个月、6个月、1年、2年。<br>**注意** 全量日志分析服务到期后，将停止存储新的日志数据。 |

6. 单击**立即购买**并完成支付。
   购买全量日志分析服务后，日志服务将自动为DDoS高防创建一个专属的日志项目（Project），用于管理DDoS高防的日志数据。您可以在日志服务控制台的首页查看DDoS高防专属日志项目。


   DDoS高防（新BGP）服务的专属日志项目名称以 `ddoscoo-project` 开头，DDoS高防（国际）服务的专属日志项目名称以 `ddosdip-project` 开头。

   DDoS高防专属日志项目默认包含以下资源：

   - 1个专属日志库（Logstore），用于存储DDoS高防的日志数据。DDoS高防（新BGP）服务的专属日志库名称为 `ddoscoo-logstore`，DDoS高防（国际）服务的专属日志库名称为 `ddosdip-logstore`。
   - 2个预设的日志仪表盘（DDoS访问中心、DDoS运营中心），用于展示日志分析图形报表。DDoS高防（新BGP）和DDoS高防（国际）服务的日志仪表盘内容相同。

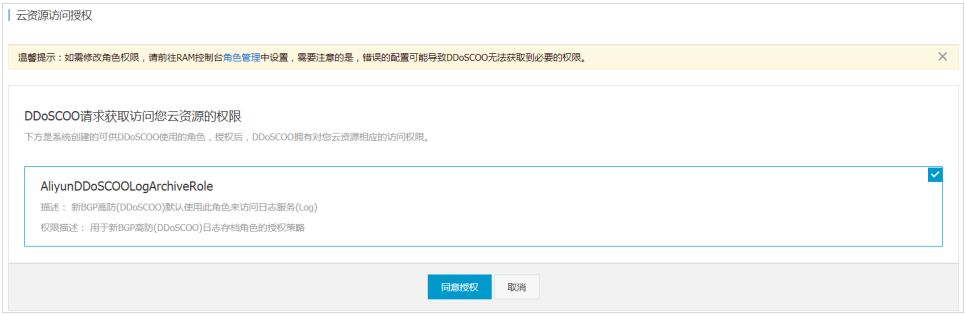
7. 返回**全量日志分析**页面，授权DDoS高防服务将日志数据存储到日志服务专属日志库。

   **说明** 您只需完成一次授权即可。如果您已经完成授权，则无需执行该步骤。

   授权步骤如下：

   i. 单击**立即授权**。

ii. 在**云资源访问授权**页面，单击**同意授权**。




成功开通全量日志分析服务并完成授权后，您就可以在**全量日志分析**页面开始使用该服务。使用全量日志分析前，您必须先为网站域名开启日志采集。相关操作，请参见步骤2：开启日志采集。

## 步骤2：开启日志采集

DDoS高防默认不采集已接入DDoS防护的网站业务的日志数据。只有当您为网站域名开启日志采集后，DDoS高防才会采集该网站的日志数据，并将采集到的日志数据存储到日志服务专属日志库中，供您进行查询与分析。

参照以下步骤，为网站域名开启日志采集：

1. 登录DDoS高防控制台。
2. 在顶部菜单栏左上角处，选择服务所在地域：
   - **中国内地**：选择该地域将跳转到**DDoS高防（新BGP）**控制台。
   - **非中国内地**：选择该地域将跳转到**DDoS高防（国际）**控制台。

     您可以通过切换地域分别管理和配置DDoS高防（新BGP）和DDoS高防（国际）实例。在使用DDoS高防服务时，请确认您已选择正确的地域。
3. 在左侧导航栏，选择**调查分析 > 全量日志分析**。
4. 在**全量日志分析**页面，为网站域名开启日志采集。

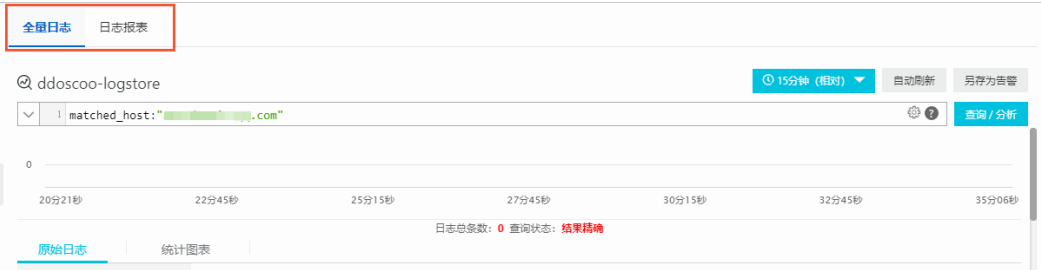
   > **注意** 网站业务必须已经完成域名接入，才可以开启日志采集。域名列表中仅显示已完成域名接入的域名。

   您可以从以下方式中选择一种，为域名开启日志采集：
   - 单独为某个域名开启日志采集：从**选择域名**下拉列表选择一个域名，打开**状态**开关。
   - 批量配置：单击页面右上方的**批量配置**，并在**批量配置**面板选中多个域名，单击**批量开启**。

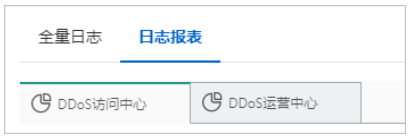

开启日志采集后，DDoS高防会采集和存储网站的日志数据，供您进行查询与分析。关于查询与分析日志的方法，请参见步骤3：使用全量日志。

## 步骤3：使用全量日志

为域名开启日志采集后，您就可以在**全量日志分析**页面，使用**全量日志**功能对采集的日志数据进行查询和分析、使用**日志报表**功能查看DDoS高防预设的日志仪表盘报表。



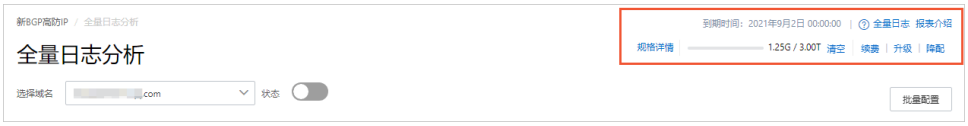

下表罗列了全量日志分析的基本功能。更多操作说明，请参见云产品日志通用操作。

| 功能 | 子功能项 | 说明 | 更多信息 |
| --- | --- | --- | --- |
| **全量日志** | 查询和分析 | 对采集到的日志数据进行实时查询分析。查询分析语句由查询语句（Search）和分析语句（Analytics）两个部分组成，查询和分析语句间使用竖线（ \| ）进行分隔。<br>例如，您可以通过以下查询分析语句，查询域名的访问量：<br>`* \| SELECT COUNT(*) as times, host GROUP by host ORDER by times desc limit 100`<br>更多查询语句示例，请参见常用查询语句示例。 | 查询和分析全量日志<br>全量日志字段说明 |
| | 分析图表 | 查询分析语句中包含分析语法，语句执行后默认按表格方式展示分析结果，您还可以选择折线图、柱状图、饼图等多种图形方式进行展示。 | 统计图表概述 |
| | 监控告警 | 您可以根据仪表盘中的查询图表设置告警，实现实时的服务状态监控。 | 告警简介 |
| **日志报表** | 仪表盘 | 仪表盘是日志服务提供的实时数据分析大盘。使用常用查询语句获取分析结果后，您可以将结果图表保存到仪表盘中。全量日志分析服务默认为您提供**DDoS访问中心**和**DDoS运营中心**两个仪表盘。<br>  <br>您还可以通过订阅仪表盘功能，通过邮件或者钉钉群消息将仪表盘内容定时推送给指定对象。 | 查询日志报表<br>订阅仪表盘 |



## 步骤4：管理服务配置

**全量日志分析**页面的右上角展示了当前全量日志分析服务的规格配置，您可以在该区域执行以下操作：



- 查询全量日志分析服务的有效期。如果全量日志分析服务即将到期，您可以通过**续费**，延长服务的有效期。

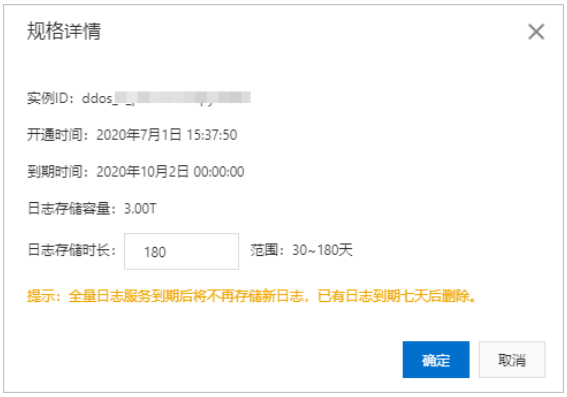
  > **警告** 全量日志分析服务到期后将不再存储新的日志数据。服务到期7天后，已有日志数据将被清空。

- 查询日志存储空间的使用情况。如果日志存储空间即将占满，您可以通过**升级**，提升日志存储空间容量；或者通过**清空**，删除不再需要保存的日志数据。

  控制台中显示的日志存储空间用量并非实时更新，与实际使用情况存在约两个小时的延迟。

  > **说明** 建议您在全量日志分析服务使用期间，定期关注全量日志存储空间的使用情况。当日志存储空间使用量超过70%时，请及时升级日志存储量规格，避免新产生的日志无法存储，影响日志存储的连续性。当日志存储空间长期空闲时，您也可以根据实际日志量的大小，降低日志存储规格。

- 修改日志存储时长。默认日志存储时长为180天。您可以单击**规格详情**，在**规格详情**对话框修改**日志存储时长**，可选范围：30~180天。




## 常用查询语句示例

- 查询拦截类型

```
* | select cc_action,cc_phase,count(*) as t group by cc_action,cc_phase order by t desc limit 10
```

- 查询QPS

```
* | select time_series(__time__,'15m','%H:%i','0') as time,count(*)/900 as QPS group by time order by time
```

- 查询被攻击域名

```
* and cc_blocks:1 | select cc_action,cc_phase,count(*) as t group by cc_action,cc_phase order by t desc limit 10
```

- 查询被攻击URL

```
* and cc_blocks:1 | select count(*) as times,host,request_path group by host,request_path order by times
```

- 查询请求详情

```
* | select date_format(date_trunc('second',__time__),'%H:%i:%s') as time,host,request_uri
,request_method,status,upstream_status,querystring limit 10
```

- 查询5XX状态码详情

```
* and status>499 | select host,status,upstream_status,count(*)as t group by host,status,u
pstream_status order by t desc
```

- 查询请求时延分布

```
* | SELECT count_if(upstream_response_time<20) as "<20",
count_if(upstream_response_time<50 and upstream_response_time>20) as "<50",
count_if(upstream_response_time<100 and upstream_response_time>50) as "<100",
count_if(upstream_response_time<500 and upstream_response_time>100) as "<500",
count_if(upstream_response_time<1000 and upstream_response_time>500) as "<1000",
count_if(upstream_response_time>1000) as ">1000"
```

# 6.2.5. 查询和分析全量日志

网站域名开启DDoS高防全量日志采集后，您可以通过全量日志页面对采集到的日志数据进行实时查询和分析。本文介绍了查询和分析DDoS高防全量日志的方法。

## 前提条件

- 已完成网站域名接入。更多信息，请参见添加网站。
- 已开通全量日志分析功能并为网站域名开启了全量日志采集。更多信息，请参见概述。

## 操作步骤

1. 登录DDoS高防控制台。
2. 在顶部菜单栏左上角处，选择服务所在地域：
   - **中国内地**：选择该地域将跳转到**DDoS高防（新BGP）**控制台。
   - **非中国内地**：选择该地域将跳转到**DDoS高防（国际）**控制台。

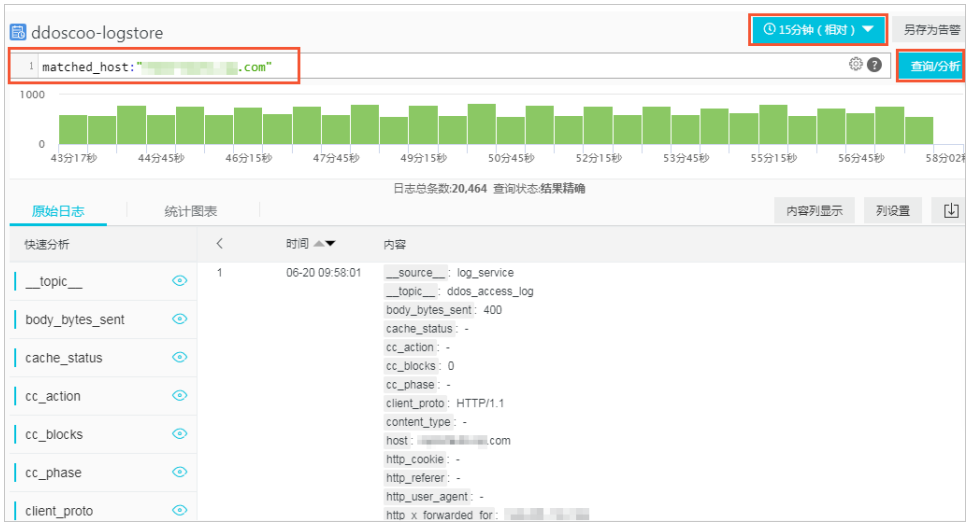
     您可以通过切换地域分别管理和配置DDoS高防（新BGP）和DDoS高防（国际）实例。在使用DDoS高防服务时，请确认您已选择正确的地域。
3. 在左侧导航栏，选择**调查分析 > 全量日志分析**。
4. 选择要查询的域名。

   > **说明** 请确认网站域名的全量日志**状态**为开启，否则无法使用相关功能。

   
   
5. 单击**15分钟（相对）**，设置查询的时间范围。

   您可以选择相对时间、整点时间和自定义时间范围。

> **说明**
>
> - DDoS高防日志的保存时间为180天，180天之前的日志数据会被删除。默认情况下只支持查询最近180天内的日志数据。
> - 查询结果相对于指定的时间范围有1分钟以内的误差。




6. 在查询框中输入查询分析语句。

   查询分析语句由查询语句和分析语句两个部分组成，通过竖线（|）进行分隔，格式：`查询语句|分析语句`。

| 语句类型 | 是否可选 | 说明 |
| --- | --- | --- |
| 查询语句 | 可选 | 查询条件，可以为查询关键词、模糊查询、数值、数值范围和组合条件。<br>如果为空或星号（*），表示针对当前时间段所有数据不设置任何过滤条件，即返回所有数据，详情请参见查询语法。<br>**说明** 关于DDoS高防访问日志的日志字段说明，请参见全量日志字段说明。 |
| 分析语句 | 可选 | 对查询结果或全量数据进行计算和统计。<br>如果为空，表示只返回查询结果，不做统计分析，详情请参见分析概述。<br>**说明**<br>- 分析语句中可以省略SQL标准语法中的`from 表格名`语句，即`from log`。<br>- 日志数据默认返回前100条，您可以通过LIMIT子句修改返回范围。 |

7. 单击**查询/分析**，查看查询分析结果。

日志服务为您提供日志分布直方图、**原始日志**和**统计图表**形式的查询分析结果，并支持设置告警、快速查询等操作。详情请参见操作查询和分析结果。

# 6.2.6. 查询日志报表

DDoS高防全量日志分析的日志报表内嵌了日志服务的仪表盘页面，为您展示DDoS高防默认仪表盘，包括DDoS访问中心和DDoS运营中心。网站域名开启DDoS高防全量日志采集后，您可以通过日志报表查询网站的DDoS高防默认仪表盘。

## 前提条件

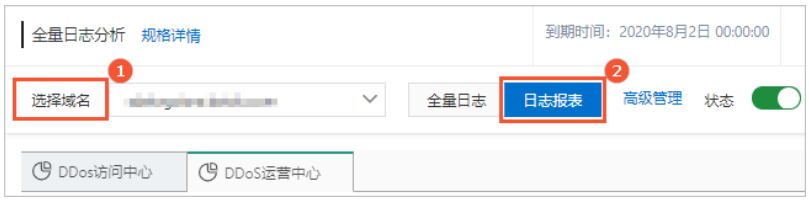
- 已完成网站域名接入。更多信息，请参见添加网站。
- 已开通全量日志分析功能并为网站域名开启了全量日志采集。更多信息，请参见概述。

## 操作步骤

1. 登录DDoS高防控制台。
2. 在顶部菜单栏左上角处，选择服务所在地域：
   - **中国内地**：选择该地域将跳转到**DDoS高防（新BGP）**控制台。
   - **非中国内地**：选择该地域将跳转到**DDoS高防（国际）**控制台。

     您可以通过切换地域分别管理和配置DDoS高防（新BGP）和DDoS高防（国际）实例。在使用DDoS高防服务时，请确认您已选择正确的地域。
3. 在左侧导航栏，选择**调查分析 > 全量日志分析**。
4. 选择要查询的域名并单击**日志报表**。

   > **说明** 请确认网站域名的全量日志**状态**为开启，否则无法使用相关功能。

   进入日志报表后，您可以看到以下DDoS高防默认仪表盘：
   - **DDoS访问中心**：展示网站的基本指标（PV、UV、流入流量、带宽峰值）、访问趋势、请求来源分布、其他统计信息（例如访问域名、客户端类型等）。
   - **DDoS运营中心**：展示网站的总体运营状况，包括带宽流入流出趋势、请求与拦截趋势、攻击者列表、被访问网站列表等。

   > **说明**
   > - 日志报表展示区域按照预定义的布局展示多个报表，包含不同的图表类型。关于图表类型的说明，请参见统计图表概述。
   > - 关于默认仪表盘包含图表的说明，请参见默认仪表盘图表说明。

5. 设置时间范围，查看DDoS高防默认仪表盘。

   日志报表中所有图表都是基于不同时间段的数据统计结果，例如访问量的默认时间范围为1小时，访问趋势为1周。如您想要设置当前页面的所有图表均按照同样的时间范围显示，则可以设置时间选择器。

i. 单击仪表盘右上角的**请选择**。

ii. 在**时间**页面设置仪表盘的时间范围。

您可以选择相对时间、整点时间或设置自定义时间。

修改时间范围后，所有图表的时间都会改成设置的时间范围。

> **说明** 时间选择器仅在当前页面提供临时的图表查看方式，系统不保存该设置。下次查看报表时，系统仍会为您展示默认的时间范围。

## 默认仪表盘图表说明

### DDoS访问中心

| 图表名称 | 类型 | 默认时间范围 | 描述 | 样例 |
| --- | --- | --- | --- | --- |
| **PV** | 单值 | 1小时（相对） | 请求总数。 | 100000 |
| **UV** | 单值 | 1小时（相对） | 独立的访问客户端的总数。 | 100000 |
| **流入流量** | 单值 | 1小时（相对） | 网站的流入流量总和，单位为MB。 | 300 MB |
| **网络in带宽峰值** | 单值 | 今天（整点时间） | 网站请求的流入流量速率的峰值，单位为Bytes/s。 | 100 Bytes/s |
| **网络out带宽峰值** | 单值 | 今天（整点时间） | 网站请求的流出流量速率的峰值，单位为Bytes/s。 | 100 Bytes/s |
| **流量带宽趋势** | 双线图 | 1周（相对） | 网站流入流出流量的趋势图，单位为KB/s。 | 无 |
| **PV/UV访问趋势** | 双线图 | 1周（相对） | PV与UV的趋势图，单位为个。 | 无 |
| **访问状态分布** | 饼图 | 1周（相对） | 各种请求处理状态（400、304、200等）的趋势图，单位为个/分钟。 | 无 |
| **访问来源** | 世界地图 | 1小时（相对） | 访问者PV在来源国家的分布。 | 无 |
| **流入流量来源（世界）** | 世界地图 | 1小时（相对） | 流入流量总和在来源国家的分布，单位为MB。 | 无 |
| **流入流量来源（中国）** | 中国地图 | 1小时（相对） | 流入流量总和在来源省份的分布，单位为MB。 | 无 |

| 图表名称 | 类型 | 默认时间范围 | 描述 | 样例 |
| --- | --- | --- | --- | --- |
| **访问热力图** | 高德地图 | 1小时（相对） | 访问者在地理位置上的访问热力图。 | 无 |
| **来源网络提供商** | 环图 | 1小时（相对） | 访问者通过网络运营商接入的流入流量分布，例如电信、联通、移动、教育网等，单位为MB。 | 无 |
| **Referer** | 表格 | 1小时（相对） | 前100个最多的跳转Referer URL、主机以及次数等。 | 无 |
| **接入线路分布** | 环图 | 1小时（相对） | 访问请求接入的DDoS高防线路的分布。 | 无 |
| **客户端类型分布** | 环图 | 1小时（相对） | 前20个被访问最多的User Agent（用户代理），例如iPhone、iPad、Widnows IE、Chrome等。 | 无 |
| **请求内容类型分布** | 环图 | 1小时（相对） | 前20个最多的请求内容类型，例如HTML、Form、JSON、流数据等。 | 无 |
| **访问域名** | 环图 | 1小时（相对） | 前20个被访问最多的域名。 | 无 |
| **访问最多的客户端** | 表格 | 1小时（相对） | 前100个访问最多的客户端信息，包括IP、PV、流入流量、错误访问次数、攻击次数等。 | 无 |
| **响应最慢的URL** | 表格 | 1小时（相对） | 前100个响应时间最长的URL信息，包括网站、URL、响应时间、访问次数等。 | 无 |

### DDoS运营中心

| 图表 | 类型 | 默认时间范围 | 描述 | 样例 |
| --- | --- | --- | --- | --- |
| **带宽流入流出（KB/S）** | 双线图 | 1周（相对） | 流入和流出带宽的趋势图。 | 无 |

| 图表 | 类型 | 默认时间范围 | 描述 | 样例 |
| --- | --- | --- | --- | --- |
| **请求与拦截** | 双线图 | 1周（相对） | 请求和拦截的攻击请求总数的趋势图。 | 无 |
| **攻击者列表** | 表格 | 1小时（相对） | 前100个攻击最多的攻击者信息，包括攻击者IP、地域信息、攻击次数和攻击总流量。 | 无 |
| **被攻击网站Top10** | 表格 | 1小时（相对） | 被攻击最多的10个网站。 | 无 |

# 6.2.7. 修改日志存储时长

DDoS高防全量日志服务默认为您存储近180天内的全量日志。您可以根据需要，在30~180范围内自定义日志存储时长。

## 前提条件

已开通DDoS高防（新BGP）或DDoS高防（国际）全量日志服务。

相关操作，请参见步骤1：开通全量日志分析。

## 背景信息

开通全量日志服务后，当日志存储容量充足且在服务有效期内，DDoS防护将从您使用服务的第一天开始，为您连续存储180天的日志数据。第181天的日志数据会覆盖第一天存储的日志数据，以此类推，始终保持存储最近180天的全量日志。

您可以根据需要，在30~180天范围内自定义日志存储时长。日志存储时长越长，同等规模业务所需的日志存储容量会越大。

如果日志存储容量已占满，新的日志数据将无法存储，会导致日志数据丢失。这种情况下，建议您升级日志存储容量。相关操作，请参见升级日志存储容量。

## 操作步骤

1. 登录DDoS高防控制台。
2. 在顶部菜单栏左上角处，选择服务所在地域：
   - **中国内地**：选择该地域将跳转到**DDoS高防（新BGP）**控制台。
   - **非中国内地**：选择该地域将跳转到**DDoS高防（国际）**控制台。

     您可以通过切换地域分别管理和配置DDoS高防（新BGP）和DDoS高防（国际）实例。在使用DDoS高防服务时，请确认您已选择正确的地域。
3. 在左侧导航栏，选择**调查分析 > 全量日志分析**。
4. 在**全量日志分析**页面右上角，单击**规格详情**。
5. 在**规格详情**对话框，设置**日志存储时长**（单位：天）。

   您可以在30~180天范围内，设置您希望存储日志的天数。


6. 单击**确定**。
   日志存储时长修改成功后，全量日志服务将只存储指定时长范围内的日志，并自动删除过期的日志。

# 6.2.8. 管理日志存储空间

开通DDoS高防全量日志服务后，您可以根据需要修改日志存储容量的规格，或清空已存储的全部日志。

## 前提条件

已开通DDoS高防（新BGP）或DDoS高防（国际）全量日志服务。

相关操作，请参见步骤1：开通全量日志分析。

## 背景信息

如果您因网站业务调整，导致所需要的日志存储容量发生变化，您可以通过升级增加日志存储容量、通过降配减小日志存储容量。例如，如果您为新的网站开启了日志采集，则日志存储容量需求会增大；如果您减少了日志存储时长，则同等规模业务的存储容量需求会相应减少。

## 如何计算所需的日志存储容量？

您可以参考以下信息，根据网站业务的日常QPS评估需要的日志存储容量：

每条请求日志大约占用2 KB存储空间，如果网站的平均请求量为500 QPS，则存储一天的日志需要的存储空间为500*60*60*24*2 = 86,400,000 KB（约82 GB）；存储180天的日志需要的存储空间为86,400,000 * 180 = 15,552,000,000 KB（约14.5 TB）。

## 日志存储容量已占满该怎么办？

如果日志存储容量已占满，新的日志数据将无法存储，会导致日志数据丢失。针对这种情况，您可以选择以下处理方法：

- （推荐）升级日志存储容量。相关操作，请参见升级日志存储容量。
- 清空已存储的日志数据，并减少日志存储时长。相关操作，请参见清空日志、修改日志存储时长。

> 注意
>
> - 日志数据只支持一次性全部清空，且清空后无法恢复。请确保您不再需要已存储的全部日志数据时，再选择该方案。
> - 每个阿里云账号总共拥有2次清空日志的机会。如需更多日志清空次数，您必须提交工单申请。我们不建议您频繁清空日志。如果日志存储容量不能满足业务需要，建议您及时升级日志存储容量。

## 升级日志存储容量

如果您确认当前的日志存储容量过小，可以通过升级增加日志存储容量。

1. 登录DDoS高防控制台。
2. 在顶部菜单栏左上角处，选择服务所在地域：
   - **中国内地**：选择该地域将跳转到**DDoS高防（新BGP）**控制台。
   - **非中国内地**：选择该地域将跳转到**DDoS高防（国际）**控制台。

     您可以通过切换地域分别管理和配置DDoS高防（新BGP）和DDoS高防（国际）实例。在使用DDoS高防服务时，请确认您已选择正确的地域。
3. 在左侧导航栏，选择**调查分析 > 全量日志分析**。
4. 在**全量日志分析**页面右上角，单击**升级**。
5. 在**变配**页面，选择一个比当前日志存储量大的**日志存储量**，并选中**全量日志服务协议**。

   示例：如果当前日志存储量为3 T，您必须选择5 T或更大的规格。
6. 单击**立即购买**，并完成支付。
   成功升级日志存储容量后，您可以在**全量日志分析**页面右上角，查看升级后的日志存储容量和使用情况。

## 降配日志存储容量

如果您确认当前的日志存储容量过大，可以通过降配减小日志存储容量。

1. 登录DDoS高防控制台。
2. 在顶部菜单栏左上角处，选择服务所在地域：
   - **中国内地**：选择该地域将跳转到**DDoS高防（新BGP）**控制台。
   - **非中国内地**：选择该地域将跳转到**DDoS高防（国际）**控制台。

     您可以通过切换地域分别管理和配置DDoS高防（新BGP）和DDoS高防（国际）实例。在使用DDoS高防服务时，请确认您已选择正确的地域。
3. 在左侧导航栏，选择**调查分析 > 全量日志分析**。
4. 在**全量日志分析**页面右上角，单击**降配**。
5. 在**降配**页面，选择一个比当前日志存储量小的**日志存储量**，并选中**全量日志服务协议**。

   示例：如果当前日志存储量为10 T，您必须选择5 T或更小的规格。
6. 单击**立即购买**，并完成支付。
   成功降配日志存储容量后，您可以在**全量日志分析**页面右上角，查看降配后的日志存储容量和使用情况。

## 清空日志

如果您不希望已存储的日志继续占用您的日志存储空间，可以清空日志。清空日志后，您当前已存储的所有日志数据将被删除。

1. 登录DDoS高防控制台。
2. 在顶部菜单栏左上角处，选择服务所在地域：
   - **中国内地**：选择该地域将跳转到**DDoS高防（新BGP）**控制台。
   - **非中国内地**：选择该地域将跳转到**DDoS高防（国际）**控制台。

     您可以通过切换地域分别管理和配置DDoS高防（新BGP）和DDoS高防（国际）实例。在使用DDoS高防服务时，请确认您已选择正确的地域。
3. 在左侧导航栏，选择**调查分析 > 全量日志分析**。
4. 在**全量日志分析**页面右上角，单击**清空**。

   > **注意** 如果日志容量的使用量为0，则不支持清空操作。

5. 在**确认清空当前全部日志**对话框，单击**确定**。

   每个阿里云账号总共拥有2次手动清空日志的机会。如果清空日志的机会已用完，您必须提交工单，申请更多的日志清空次数。我们不建议您频繁清空日志。如果日志存储容量不能满足业务需要，建议您及时升级日志存储容量。

   > **警告** 日志数据清空后，将无法恢复。请谨慎操作。

   清空日志后，您需要等待2～3个小时，才可以在**全量日志分析**页面右上角查看日志清空的结果。

# 6.2.9. 续费全量日志服务

DDoS高防全量日志服务到期后，将不再存储新的日志数据，已存储的日志会在服务到期7天后被自动清空（无法恢复）。为避免全量日志服务到期给您的业务带来影响，建议您关注服务到期时间并及时为服务手动续费，或开通自动续费。

## 前提条件

已开通DDoS高防（新BGP）或DDoS高防（国际）全量日志服务。

相关操作，请参见步骤1：开通全量日志分析。

## 查询服务到期时间

1. 登录DDoS高防控制台。
2. 在顶部菜单栏左上角处，选择服务所在地域：
   - **中国内地**：选择该地域将跳转到**DDoS高防（新BGP）**控制台。
   - **非中国内地**：选择该地域将跳转到**DDoS高防（国际）**控制台。

     您可以通过切换地域分别管理和配置DDoS高防（新BGP）和DDoS高防（国际）实例。在使用DDoS高防服务时，请确认您已选择正确的地域。
3. 在左侧导航栏，选择**调查分析 > 全量日志分析**。
4. 在**全量日志分析**页面右上角，单击**规格详情**。
5. 在**规格详情**对话框，查看全量日志服务的**到期时间**。


## 手动续费

1. 登录DDoS高防控制台。
2. 在顶部菜单栏左上角处，选择服务所在地域：
   - **中国内地**：选择该地域将跳转到**DDoS高防（新BGP）**控制台。
   - **非中国内地**：选择该地域将跳转到**DDoS高防（国际）**控制台。

     您可以通过切换地域分别管理和配置DDoS高防（新BGP）和DDoS高防（国际）实例。在使用DDoS高防服务时，请确认您已选择正确的地域。
3. 在左侧导航栏，选择**调查分析 > 全量日志分析**。
4. 在**全量日志分析**页面右上角，单击**续费**。
5. 在**续费**页面，选择**购买时长**，并选中**全量日志服务协议**。
6. 单击**立即购买**，并完成支付。
   成功续费后，您可以在**全量日志分析**页面，通过**规格详情**查看更新后的**到期时间**。

## 开通自动续费

1. 登录DDoS高防控制台。
2. 在顶部菜单栏，选择**费用 > 续费管理**。
3. 在**手动续费**页签，定位到要续费的**全量日志**实例，单击**操作**下的**开通自动续费**。


4. 在**开通自动续费**对话框，选择**自动续费周期**，并单击**开通自动续费**。


示例：**自动续费周期**设置为**3个月**，则阿里云将在服务到期时，自动为您延长3个月的服务时长，并从您的阿里云账号余额中自动扣除相关费用。

成功开通自动续费后，您可以在**自动续费**页签下查看自动续费配置，并可以执行**恢复手动续费**操作。

# 6.3. 查询操作日志

如果您使用DDoS高防（新BGP）服务，则您可以在DDoS高防控制台的操作日志页面查看近180天的重要操作日志。

## 前提条件

已购买DDoS高防（新BGP）实例。

> **注意** 只有DDoS高防（新BGP）服务支持查询操作日志，DDoS高防（国际）不支持该功能。

## 背景信息

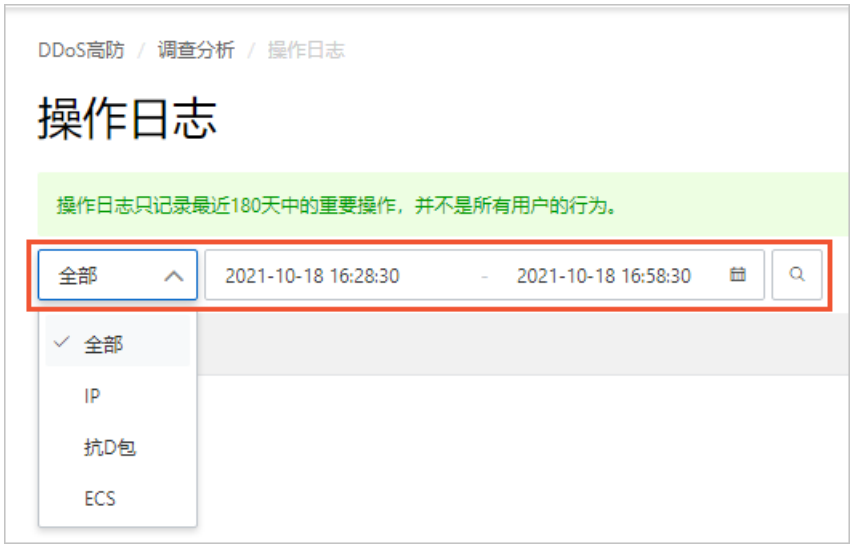
操作日志只记录最近180天中的重要操作，并非记录所有用户行为。

DDoS高防（新BGP）支持的操作日志类型如下：

- 实例购买成功、实例释放
- ECS实例更换IP
- 黑洞解封操作
- 流量封禁和解封操作
- 四层流量清洗模式变更操作
- CC防护模式变更操作
- 弹性防护带宽变更操作

## 操作步骤

1. 登录DDoS高防控制台。
2. 在顶部菜单栏左上角处，选择**中国内地**地域。
   选择该地域将跳转到**DDoS高防（新BGP）**控制台。
3. 在左侧导航栏，选择**调查分析 > 操作日志**。
4. 在**操作日志**页面，设置要查看的操作日志类型（**全部**、**IP**、**抗D包**、**ECS**）和时间范围，查看对应数据。




# 6.4. 查询系统日志

您可以通过系统日志页面查询DDoS高防实例的弹性业务带宽账单。

## 前提条件

- 已购买DDoS高防（新BGP）实例。

  相关操作，请参见购买DDoS高防实例。
- 已为DDoS高防实例开启弹性业务带宽。

  相关操作，请参见设置弹性业务带宽。

## 背景信息

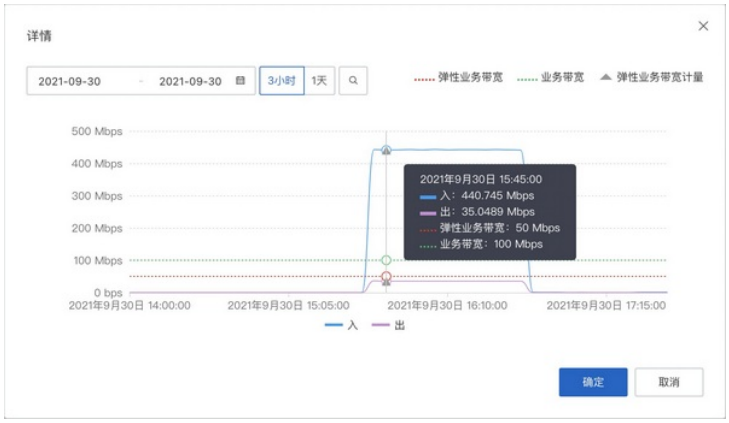
**系统日志**页面支持查询最近180天内DDoS高防的系统事件记录（目前只包含弹性业务带宽账单）。

启用弹性业务带宽后，您可以通过**系统日志**页面查询最近180天内的弹性业务带宽账单。关于弹性业务带宽的计费方式说明，请参见弹性业务带宽计费方式。

## 操作步骤

1. 登录DDoS高防控制台。
2. 在顶部菜单栏左上角处，选择**中国内地**地域。
   选择该地域将跳转到**DDoS高防（新BGP）**控制台。
3. 在左侧导航栏，选择**调查分析 > 系统日志**。
4. 在**系统日志**页面，设置查询时间范围，查询对应的弹性业务带宽账单。

   账单的**状态**包含：
   - **待出账**：表示该账单仍未正式出账。您可以单击**详情**列下的**查看**，通过**详情**对话框查询上个计费月份内的实际业务流量详情（如下图所示）。




**详情**对话框支持快速查询最近3小时、1天的实际业务流量数据，具体说明如下：

- 蓝色实线和紫色实线分别表示入方向、出方向的实际业务流量峰值。
- 绿色虚线和红色虚线分别表示DDoS高防实例的业务带宽规格（上图中为100 Mbps）、已启用的弹性业务带宽大小（上图中为50 Mbps）。
- 使用灰色三角形标识的竖线表示计费月份的弹性业务带宽用量计量点。以上图为例，取入方向和出方向流量峰值中的较大者，即入方向流量峰值440.745 Mbps。

- **终止出账**：表示该账单已结束出账（不产生实际费用）。
- **已出账**：表示该账单已按照实际弹性业务带宽用量正式出账。

# 6.5. 查看高级防护日志

如果您使用DDoS高防（国际）服务，则您可以在DDoS高防控制台的高级防护日志页面查看近30天的全局高级防护记录。

## 前提条件

已开通DDoS高防（国际）实例。

## 操作步骤

1. 登录DDoS高防控制台。
2. 在顶部导航栏，选择**非中国内地**地域。
3. 在左侧导航栏，选择**调查分析 > 高级防护日志**。
4. 在**高级防护日志**页面，选择要查询的实例和时间范围，查看对应数据。

# 6.6. 云监控告警

## 6.6.1. 设置云监控告警

您可以使用云监控的报警服务功能，针对DDoS高防的常用业务指标（例如，高防IP流量、连接数等）、攻击事件（例如，黑洞、清洗事件）设置告警规则，使云监控在高防上业务发生异常时，及时向您发送告警，帮助您缩短响应时间，尽快恢复业务。

云监控（CloudMonitor）是一项针对阿里云资源和互联网应用进行监控的服务。关于云监控的更多介绍，请参见什么是云监控。

### 前提条件

已购买DDoS高防（新BGP、国际）实例。相关操作，请参见购买DDoS高防实例。

### 操作步骤

1. 登录DDoS高防控制台。
2. 在顶部菜单栏左上角处，选择服务所在地域：
   - **中国内地**：选择该地域将跳转到**DDoS高防（新BGP）**控制台。
   - **非中国内地**：选择该地域将跳转到**DDoS高防（国际）**控制台。

     您可以通过切换地域分别管理和配置DDoS高防（新BGP）和DDoS高防（国际）实例。在使用DDoS高防服务时，请确认您已选择正确的地域。
3. 在左侧导航栏，选择**调查分析 > 云监控告警**。
4. 在**云监控告警**页面，根据您要设置的告警类型，单击**联动配置**列下对应的**云监控通知**。


   - 如果您想要设置**IP流量告警**、**连接数告警**、**QPS告警**、**状态码告警**，单击对应的**云监控通知**。

     页面将会跳转到云监控控制台的**报警服务**页面，您可以在该页面为DDoS高防（新BGP、国际）创建阈值报警规则。相关操作，请参见设置DDoS高防报警规则。
   - 如果您想要设置**DDoS黑洞事件告警**、**DDoS清洗事件告警**，单击对应的**云监控通知**。

     页面将会跳转到云监控控制台的**事件监控**页面，您可以在该页面为DDoS高防（新BGP、国际）创建事件报警规则。相关操作，请参见设置DDoS高防事件报警。
   - 如果您想要设置**DDoS监控大盘**，单击对应的**云监控通知**。

     页面将会跳转到云监控控制台的**自定义大盘**页面，您可以在该页面为DDoS高防（新BGP、国际）创建监控大盘和添加图表。相关操作，请参见创建DDoS高防监控大盘。

# 6.6.2. 设置DDoS高防报警规则

本实践介绍了使用阿里云云监控配置DDoS高防（新BGP、国际）报警通知的操作方法。通过设置DDoS高防报警通知，您可以及时获知高防IP上的流量和连接异常情况，并在发生故障时第一时间发现问题，缩短故障处理时间，以便尽快恢复业务。

## 背景信息

云监控（CloudMonitor）是一项针对阿里云资源和互联网应用进行监控的服务。云监控为您提供监控数据的报警功能。您可以通过设置报警规则来定义报警系统如何检查监控数据，并在监控数据满足报警条件时发送报警通知。您对重要监控指标设置报警规则后，便可在第一时间得知指标数据发生的异常，迅速处理故障。更多信息，请参见概览。

云监控报警功能兼容DDoS高防（新BGP、国际），您可以在云监控中配置DDoS高防的报警通知规则。

下表描述了云监控支持监控的DDoS高防（新BGP、国际）的数据指标。

| 监控项 | 监控维度 | 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回源流量（通过高防清洗后回源到源站服务器的干净业务流量） | 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 |
| 活跃连接数 | 实例维度、IP维度 | 个 |
| 非活跃连接数 | 实例维度、IP维度 | 个 |
| 新建连接数 | 实例维度、IP维度 | 个 |
| QPS | 域名维度 | 个/秒 |
| QPS环比下降率 | 域名维度 | % |
| QPS环比增长率 | 域名维度 | % |
| 2XX状态码数量 | 域名维度 | 个 |
| 2XX状态码占比 | 域名维度 | % |
| 3XX状态码数量 | 域名维度 | 个 |
| 3XX状态码占比 | 域名维度 | % |
| 404状态码数量 | 域名维度 | 个 |
| 404状态码占比 | 域名维度 | % |
| 4XX状态码数量 | 域名维度 | 个 |

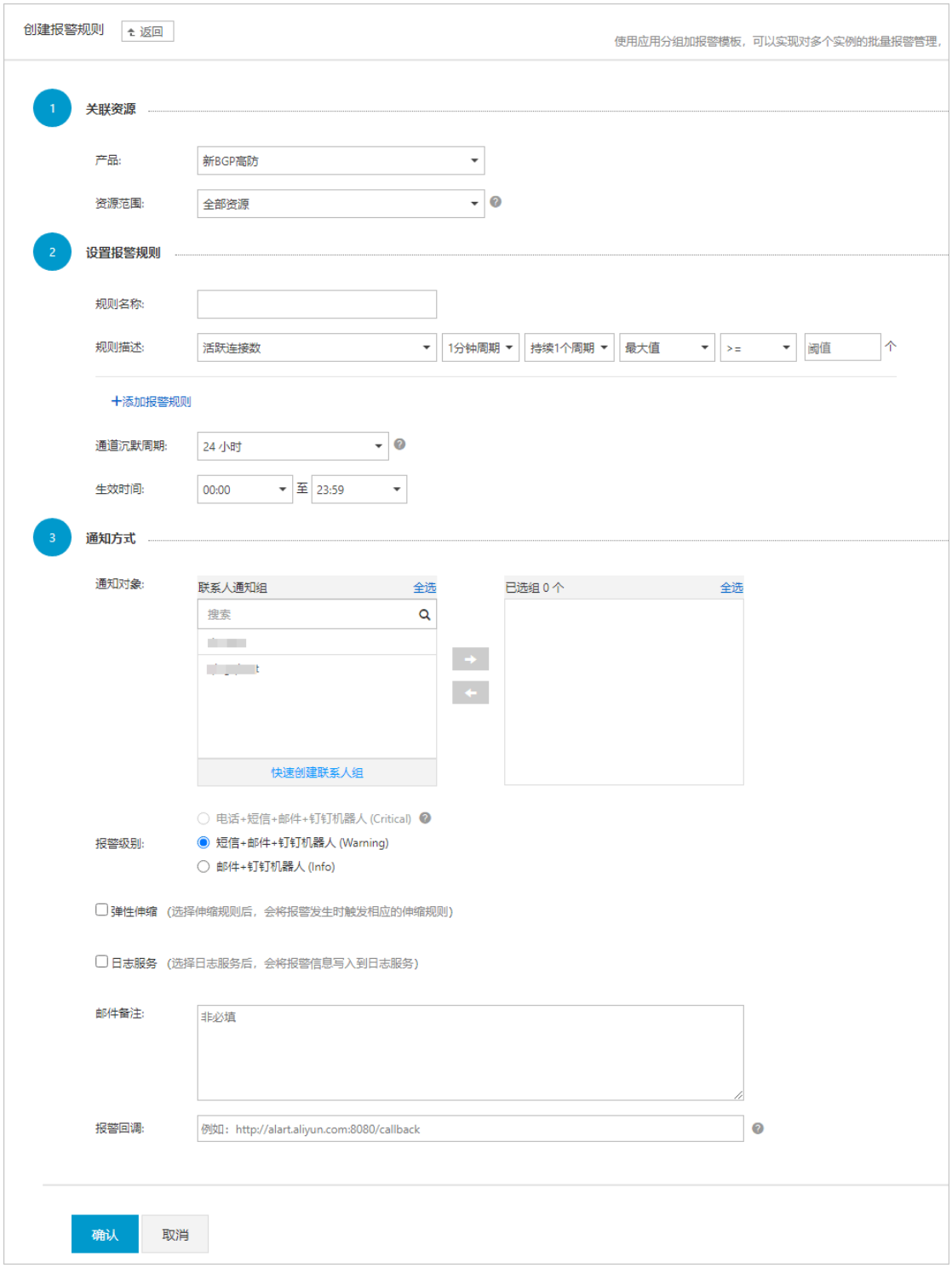
| 监控项 | 监控维度 | 单位 |
| --- | --- | --- |
| 4XX状态码占比 | 域名维度 | % |
| 5XX状态码数量 | 域名维度 | 个 |
| 5XX状态码占比 | 域名维度 | % |
| 2XX回源状态码数量 | 域名维度 | 个 |
| 2XX回源状态码占比 | 域名维度 | % |
| 3XX回源状态码数量 | 域名维度 | 个 |
| 3XX回源状态码占比 | 域名维度 | % |
| 404回源状态码数量 | 域名维度 | 个 |
| 404回源状态码占比 | 域名维度 | % |
| 4XX回源状态码数量 | 域名维度 | 个 |
| 4XX回源状态码占比 | 域名维度 | % |
| 5XX回源状态码数量 | 域名维度 | 个 |
| 5XX回源状态码占比 | 域名维度 | % |

## 操作步骤

1. 登录云监控控制台。
2. （可选）创建报警联系人。如果已有联系人，请跳过此步骤。
   i. 在左侧导航栏，选择**报警服务 > 报警联系人**。
   ii. 在**报警联系人**页签，单击**新建联系人**。
   iii. 在**设置报警联系人**面板，填写联系人信息并完成滑块验证，单击**确认**。
3. （可选）创建报警联系组。如果已有联系人组，请跳过此步骤。

   **说明** 报警通知的接收对象必须是联系人组，您可以在联系人组中添加一个或多个联系人。

   i. 在左侧导航栏，选择**报警服务 > 报警联系人**。
   ii. 在**报警联系组**页签，单击**新建联系组**。
   iii. 在**新建联系组**面板，设置**组名**，从**已有联系人**中选择并添加联系人到当前组，单击**确认**。
4. 创建报警规则。
   i. 在左侧导航栏，选择**报警服务 > 报警规则**。
   ii. 在**阈值报警**页签，单击**创建报警规则**。
   iii. 在**创建报警规则**页面，完成报警规则配置，并单击**确认**。




报警规则的配置描述如下。

| 类型 | 参数 | 说明 |
| --- | --- | --- |
| | **产品** | 选择**新BGP高防**或者**DDoS高防国际**。 |

| 类型<br>关联资源 | 参数 | 说明 |
| --- | --- | --- |
| | **资源范围** | 报警规则的作用范围，分为**全部资源**、**实例**。<br>■ **全部资源**：资源范围选择全部资源，则所有DDoS新BGP或者国际高防实例满足报警规则描述时，都会发送报警通知。<br>■ **实例**：资源范围选择指定的实例，则选中的DDoS新BGP或者国际高防实例满足报警规则描述时，才会发送报警通知。 |
| **设置报警规则** | **规则名称** | 报警规则的名称。 |
| | **规则描述** | 报警规则的内容，定义在监控数据满足何种条件时，触发报警规则。<br>**说明** 建议您根据实际业务情况设置各项监控指标（参见DDoS高防监控指标）的报警阈值。阈值太低会频繁触发报警，影响监控服务体验。阈值太高，在触发阈值后没有足够的预留时间来响应和处理攻击。<br>报警规则举例说明：<br>■ 规则描述设置为 **新建连接数** \| 5**分钟周期** \| **连续**3**周期** \| **只要有一次** \| > \| 200**个** ，表示报警服务会探测任意连续3个周期的新建连接数数据（单个DDoS高防监控指标60秒上报一个数据点，5分钟有5个数据点，连续3个周期有15个数据点），只要有一次大于200个，结果就符合报警规则，发送报警通知。<br>■ 规则描述设置为 **高防**IP**出流量** \| 5**分钟周期** \| **连续**3**周期** \| **只要有一次** \| ≥ \| 50 Mbit/s ，表示报警服务会探测任意连续3个周期的高防IP出流量数据（单个DDoS高防监控指标60秒上报一个数据点，5分钟有5个数据点，连续3个周期有15个数据点），只要有一次大于等于50 Mbit/s，结果就符合报警规则，发送报警通知。<br>单击**添加报警规则**，可以添加多个规则，每个规则单独设置**规则名称**和**规则描述**。<br>  |
| | **通道沉默周期** | 报警发生后如果未恢复正常，间隔多久重复发送一次报警通知。最短为5分钟，最长为24小时。 |
| | **生效时间** | 报警规则的生效时间，报警规则只在生效时间内发送报警通知，非生效时间内产生的报警只记录报警历史。 |

| 类型 | 参数 | 说明 |
| --- | --- | --- |
| 通知方式 | **通知对象** | 接收报警通知的联系人组。 |
| | **报警级别** | 分为Critical 、Warning、Info三个级别，不同级别对应不同的通知方式。<br>■ 电话+短信+邮件+钉钉机器人（Critical）<br>说明 购买云监控电话报警资源包后才可以选择。<br>■ 短信+邮件+钉钉机器人（Warning）<br>■ 邮件+钉钉机器人（Info） |
| | **弹性伸缩** | 选择弹性伸缩规则后，云监控会在报警发生时触发相应的弹性伸缩规则。 |
| | **日志服务** | 选择日志服务后，云监控会将报警信息写入到日志服务。 |
| | **邮件备注** | 自定义报警邮件补充信息，非必填。填写邮件备注后，发送报警的邮件通知中会附带您的备注。 |
| | **报警回调** | 云监控会将报警信息通过POST请求推送到您填写的公网URL地址，目前仅支持HTTP协议。 |

成功创建DDoS高防报警规则后，当DDoS高防监控指标满足报警条件时，报警联系人组会按照规则中指定的通知方式收到报警通知。

# 6.6.3. 设置DDoS高防事件报警

本文介绍了使用阿里云云监控配置DDoS高防（新BGP、国际）黑洞、清洗、CC攻击（四层、七层）事件报警通知的方法。通过为DDoS高防配置事件报警，您能够及时获知高防IP上的攻击事件，并在发生故障时第一时间发现问题，缩短故障处理时间，以便尽快恢复业务。

## 背景信息

云监控（CloudMonitor） 是一项针对阿里云资源和互联网应用进行监控的服务。云监控支持事件监控功能，为您提供各类云产品产生的系统事件的统一查询和统计入口，使您明确知晓云产品的使用状态，让云更透明。

您可以通过事件监控查询DDoS高防实例（新BGP、国际）上发生的黑洞、清洗、四层CC攻击、七层CC攻击事件，并为DDoS高防添加相关事件的报警通知。事件监控支持根据事件等级配置报警，通过短信、邮件、钉钉等接收通知或设置报警回调，使您第一时间知晓严重事件并及时进行处理，形成线上自动化运维闭环。更多信息，请参见事件监控概览。

## 操作步骤

1. 登录云监控控制台。
2. （可选）创建报警联系人。如果已有联系人，请跳过此步骤。
   i. 在左侧导航栏，选择**报警服务 > 报警联系人**。

ii. 在**报警联系人**页签，单击**新建联系人**。

iii. 在**设置报警联系人**面板，填写联系人信息并完成滑块验证，单击**确认**。

3. （可选）创建报警联系组。如果已有联系人组，请跳过此步骤。

> **说明** 报警通知的接收对象必须是联系人组，您可以在联系人组中添加一个或多个联系人。

i. 在左侧导航栏，选择**报警服务 > 报警联系人**。

ii. 在**报警联系组**页签，单击**新建联系组**。

iii. 在**新建联系组**面板，设置**组名**，从**已有联系人**中选择并添加联系人到当前组，单击**确认**。

4. 创建云产品事件报警规则。

i. 在左侧导航栏，单击**事件监控**。

ii. 在**报警规则**页签，选择**系统事件**，并单击**创建事件报警**。

iii. 在**创建/修改事件报警**面板，完成报警配置，并单击**确定**。

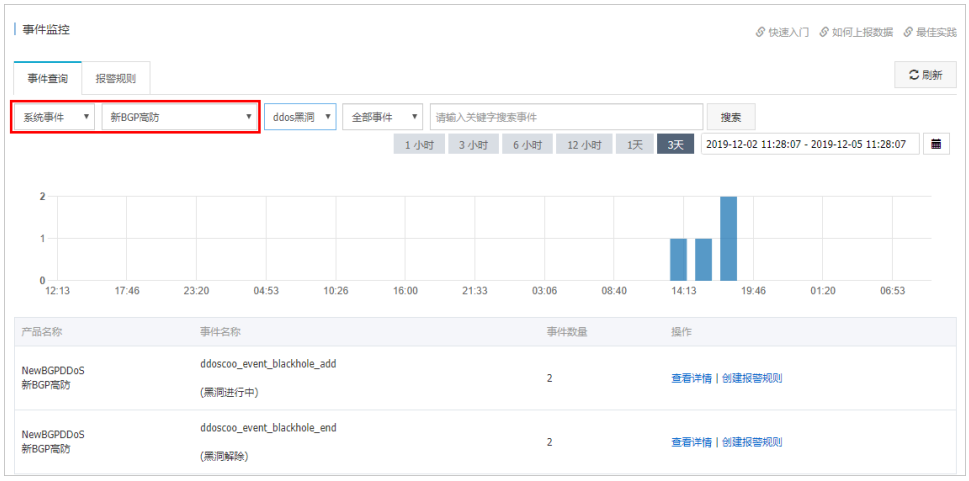

| 类型 | 配置项 | 说明 |
| --- | --- | --- |
| **基本信息** | **报警规则名称** | 为报警规则命名。 |
| | **事件类型** | 选择**系统事件**。 |
| | **产品类型** | 选择**新BGP高防**、**DDoS高防国际**。 |

| 类型 | 配置项 | 说明 |
| --- | --- | --- |
| 事件报警规则 | 事件类型 | 选择要通知的事件类型。可选项：<br>■ **ddos黑洞**：表示DDoS攻击黑洞事件。<br>■ **ddos清洗**：表示DDoS攻击清洗事件。<br>■ **ddos4层cc攻击**：表示四层CC攻击事件。<br>■ **ddos7层cc攻击**：表示七层CC攻击事件。 |
| | 事件等级 | 选择要通知的事件等级。可选项：**严重**、**警告**、**信息**。<br>**注意** 所有DDoS告警事件均为严重等级，该参数必须包含**严重**。 |
| | 事件名称 | 选择要通知的事件。不同事件类型包含的事件不同，具体说明如下：<br>■ DDoS攻击黑洞事件包括：**黑洞进行中**、**黑洞解除**。<br>■ DDoS攻击清洗事件包括：**清洗进行中**、**清洗解除**。<br>■ 四层CC攻击事件包括：**4层cc攻击进行中**、**4层cc攻击结束**。<br>■ 七层CC攻击事件包括：**7层cc攻击进行中**、**7层cc攻击结束**。 |
| | 资源范围 | 选择**全部资源**。 |
| 报警方式 | 报警通知 | 选中**报警通知**，并设置**联系人组**和**通知方式**。<br>■ 联系人组：选择一个已有联系人组。<br>■ 通知方式：选择**Warning（短息+邮箱+钉钉机器人）**或者**Info（邮箱+钉钉机器人）**方式。<br>单击**添加操作**，可以设置多个联系人组和通知方式。 |
| | 消息服务队列 | 无需设置。 |
| | 函数计算 | 无需设置。 |
| | URL回调 | 无需设置。 |
| | 日志服务 | 无需设置。 |

成功创建DDoS高防事件监控报警规则后，当DDoS高防实例上发生报警事件时，报警规则中指定的联系人组会收到报警通知 。

5. （可选）查询事件。您可以在云监控查询近期发生的DDoS报警事件。
   i. 前往**事件监控**页面，并打开**事件查询**页签。

ii. 选择**系统事件**和**新BGP高防**或者**DDoS高防国际**产品，并设置要查询的事件类型和时间范围，查询相关历史事件。




iii. 在历史事件记录中，您可以单击事件后的**查看详情**，展开查看事件详情。


# 6.6.4. 创建DDoS高防监控大盘

本实践介绍了使用阿里云云监控创建和自定义DDoS高防（新BGP&国际）实时监控大盘和数据图表的操作方法。自定义DDoS高防监控大盘和数据图表能够帮助您直观、全面地了解DDoS高防的业务防护情况。

## 背景信息

云监控（CloudMonitor） 是一项针对阿里云资源和互联网应用进行监控的服务。云监控的Dashboard功能为您提供自定义查看监控数据的功能。您可以在一张监控大盘中跨产品、跨实例查看监控数据，将相同业务的不同产品实例集中展现。更多信息，请参见概览。

云监控Dashboard功能兼容DDoS高防，您可以在云监控中配置DDoS高防（新BGP&国际）监控大盘。

下表描述了云监控支持监控的DDoS高防（新BGP&国际）的数据指标。

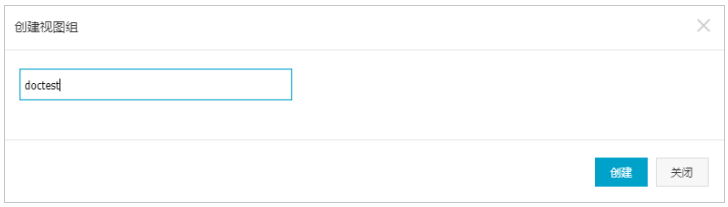
| 监控项 | 监控维度 | 单位 |
| --- | --- | --- |
| 高防IP出流量 | 实例维度、IP维度 | bit/s |
| 高防IP入流量 | 实例维度、IP维度 | bit/s |
| 高防IP回源流量（通过高防清洗后回源到源站服务器的干净业务流量） | 实例维度、IP维度 | bit/s |
| 高防IP攻击流量 | 实例维度、IP维度 | bit/s |

| 监控项 | 监控维度 | 单位 |
| --- | --- | --- |
| 活跃连接数 | 实例维度、IP维度 | 个 |
| 非活跃连接数 | 实例维度、IP维度 | 个 |
| 新建连接数 | 实例维度、IP维度 | 个 |
| QPS | 域名维度 | 个/秒 |
| QPS环比下降率 | 域名维度 | % |
| QPS环比增长率 | 域名维度 | % |
| 2XX状态码数量 | 域名维度 | 个 |
| 2XX状态码占比 | 域名维度 | % |
| 3XX状态码数量 | 域名维度 | 个 |
| 3XX状态码占比 | 域名维度 | % |
| 404状态码数量 | 域名维度 | 个 |
| 404状态码占比 | 域名维度 | % |
| 4XX状态码数量 | 域名维度 | 个 |
| 4XX状态码占比 | 域名维度 | % |
| 5XX状态码数量 | 域名维度 | 个 |
| 5XX状态码占比 | 域名维度 | % |
| 2XX回源状态码数量 | 域名维度 | 个 |
| 2XX回源状态码占比 | 域名维度 | % |
| 3XX回源状态码数量 | 域名维度 | 个 |
| 3XX回源状态码占比 | 域名维度 | % |
| 404回源状态码数量 | 域名维度 | 个 |
| 404回源状态码占比 | 域名维度 | % |
| 4XX回源状态码数量 | 域名维度 | 个 |
| 4XX回源状态码占比 | 域名维度 | % |
| 5XX回源状态码数量 | 域名维度 | 个 |
| 5XX回源状态码占比 | 域名维度 | % |

## 操作步骤

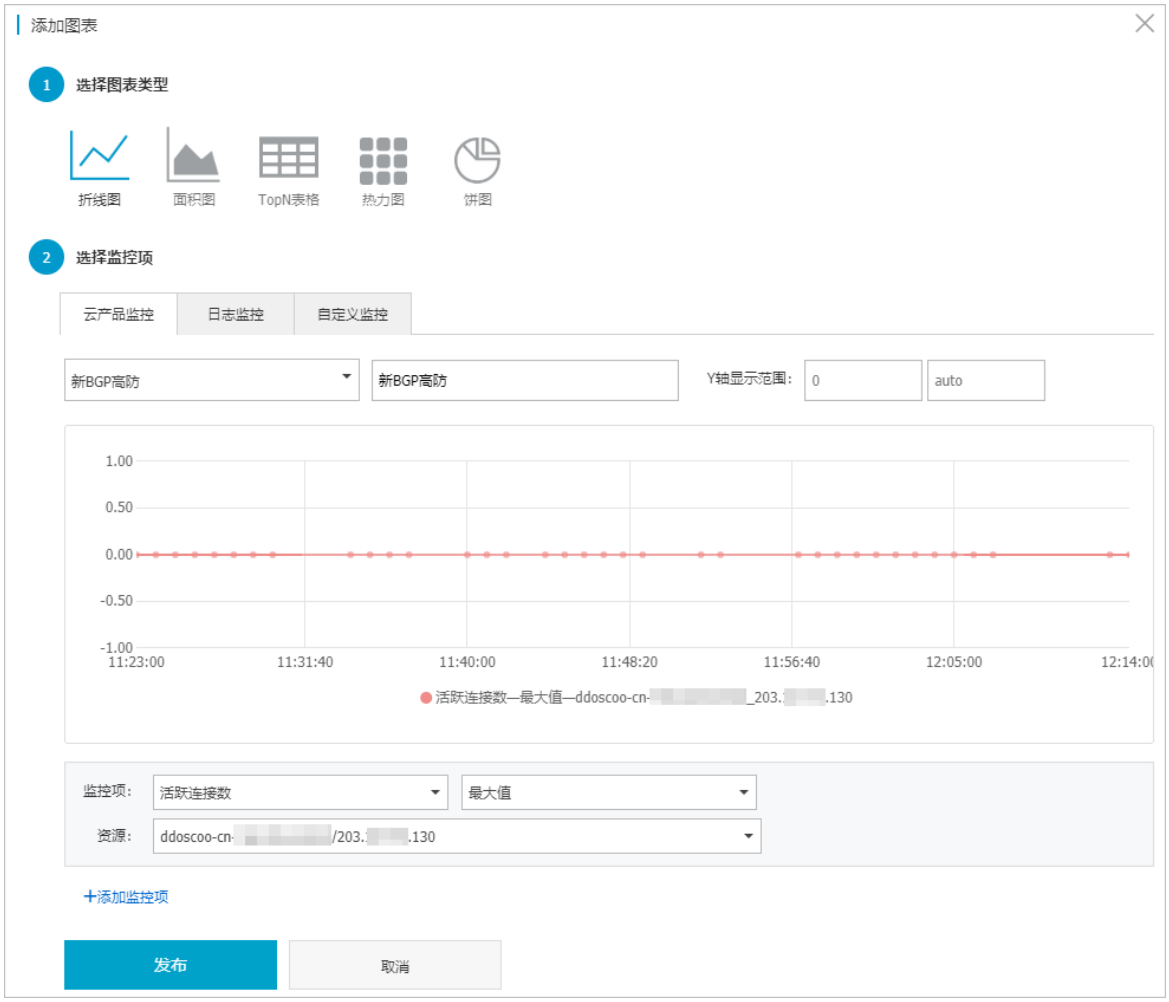
1. 登录云监控控制台。
2. 在左侧导航栏，选择**Dashboard > 自定义大盘**。
3. 单击**创建监控大盘**。


4. 在**创建视图组**对话框，设置大盘名称并单击**创建**。




成功添加监控大盘后，页面跳转到新建的监控大盘。您可以通过**当前监控大盘**选项切换要查看或操作的监控大盘。

5. 单击**添加图表**，并在**添加图表**页面自定义图表内容。

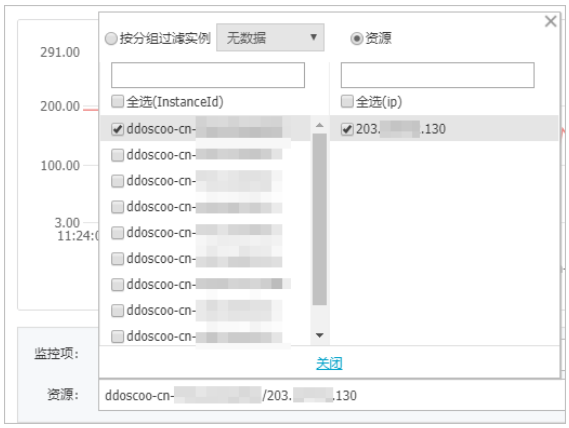



i. **选择图表类型**。支持的类型包括折线图、面积图、TopN表格、热力图、饼图。

   关于不同图表类型的具体说明，请参见管理自定义大盘中的监控图表。

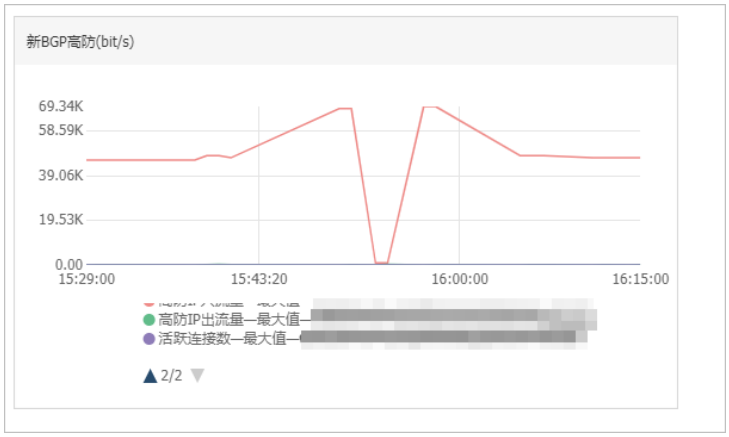
ii. **选择监控项**。选择**云产品监控**，并设置产品为**新BGP高防**或者**DDoS高防国际**，进一步配置**监控项**和**资源**。

   - 监控项：选择要监控的DDoS高防数据指标。详细信息，请参见DDoS高防监控指标。
   - 资源：选择要监控的DDoS高防实例和IP。




单击**添加监控项**可以在当前图表中添加多个监控项。

iii. 单击**发布**，生成监控图表。




成功生成监控图表后，您可以重复该步骤，在当前监控大盘下继续添加更多的图表。

# 7.防护设置

# 7.1. 基础设施DDoS防护

## 7.1.1. 设置黑白名单（针对高防实例IP）

黑白名单（针对高防实例IP）表示针对访问DDoS高防实例的请求来源IP设置的封禁或者放行规则。DDoS高防实例会丢弃来自黑名单IP的流量，放行来自白名单IP的流量。本文介绍了手动设置黑白名单的操作方法。

### 前提条件

已开通DDoS高防（新BGP）或DDoS高防（国际）实例。相关操作，请参见购买DDoS高防实例。

### 背景信息

黑白名单（针对高防实例IP）对单个DDoS高防实例生效。您可以通过设置黑白名单（针对高防实例IP），查询生效的黑白名单IP、手动添加黑白名单IP、清空已有黑白名单IP、下载黑白名单IP。

黑名单IP的访问流量将被DDoS高防实例直接丢弃。黑名单IP存在有效期，具体说明如下：

- 手动添加黑名单IP时，您需要指定其有效期。最短可以设置5分钟，最长可以设置7天。
- 黑名单中包含DDoS高防智能防御算法标记的恶意IP。如果是智能防御算法标记的恶意IP，其有效期由智能防御算法动态计算，最短5分钟，最长1小时。如果恶意IP在有效期内有持续的恶意攻击行为，DDoS高防将自动延长有效期。

白名单IP的访问流量将被DDoS高防实例直接放行。白名单IP永久生效。

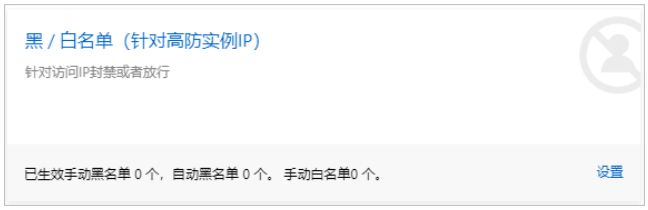
如果黑名单和白名单中的IP出现冲突，遵循白名单优先原则。如果某个IP已经在白名单中，则无法被添加到黑名单中；这种情况下，您必须先将该IP从白名单中移除，才能将该IP添加到黑名单中。

### 操作步骤

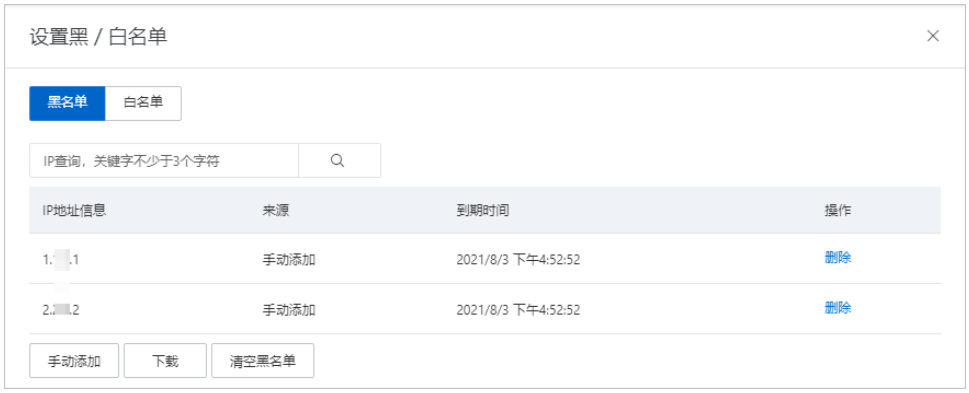
1. 登录DDoS高防控制台。
2. 在顶部菜单栏左上角处，选择服务所在地域：
   - **中国内地**：选择该地域将跳转到**DDoS高防（新BGP）**控制台。
   - **非中国内地**：选择该地域将跳转到**DDoS高防（国际）**控制台。

     您可以通过切换地域分别管理和配置DDoS高防（新BGP）和DDoS高防（国际）实例。在使用DDoS高防服务时，请确认您已选择正确的地域。
3. 在左侧导航栏，选择**防护设置 > 通用防护策略**。
4. 在**基础设施DDoS防护**页签，从左侧实例列表中选择要设置的DDoS高防实例。

   您可以使用实例ID、实例备注搜索目标实例。
5. 定位到**黑/白名单（针对高防实例IP）**区域，单击**设置**。




6. 在**设置黑/白名单**面板，单击**黑名单**或**白名单**，分别管理黑名单、白名单。




- 关于黑名单管理的具体操作，请参见步骤7。
- 关于白名单管理的具体操作，请参见步骤8。

7. 管理黑名单。
   - 手动添加黑名单IP
     a. 单击**手动添加**。

        黑名单中最多支持手动添加2000个IP。多个IP地址间使用空格或换行方式分隔。

     b. 在**黑名单配置**对话框，输入要封禁的请求来源IP并选择**黑名单有效期**。

        **黑名单有效期**最短可以设置5分钟，最长可以设置7天。支持自定义黑名单有效期，单位：秒。


     c. 单击**添加**。

     成功添加黑名单IP后，黑名单IP在有效期内的所有访问请求将被丢弃。有效期过后，黑名单IP将从黑名单配置中自动移除；如果您还需要丢弃该IP的访问请求，可以重新将该IP添加为黑名单IP。
   - 搜索黑名单IP：在搜索框中输入IP关键字，单击查询图标，即可查询黑名单中符合条件的IP。
   - 清空黑名单：单击**清空黑名单**，将当前黑名单中的所有IP移除。您也可以单击某个IP后的**删除**，单独将其从黑名单中移除。
   - 下载黑名单
     a. 单击**下载**，下发黑名单导出任务。
     b. 在导出任务已下发提示中，单击**确定**。
     c. 关闭**设置黑/白名单**页面，返回上一级页面。
     d. 单击页面右上角的图标，展开任务列表。
     e. 定位到黑名单导出任务，等待**任务状态**变为**已完成**，单击**操作**列下的**下载**。

成功下载黑名单IP到本地计算机后，您可以打开下载的TXT文件，查看黑名单明细。

8. 管理白名单。
   - 手动添加白名单IP
     a. 单击**手动添加**。
     b. 在**白名单配置**对话框，输入要放行的请求来源IP。

     > **说明** 白名单中最多支持手动添加2000个IP。多个IP地址间使用空格或换行方式分隔。

     c. 单击**添加**。

     成功添加白名单IP后，白名单IP永久有效，其所有访问请求均直接放行。
   - 搜索白名单IP：在搜索框中输入IP关键字，单击查询图标，即可查询白名单中符合条件的IP。
   - 清空白名单：单击**清空白名单**，将当前白名单中的所有IP移除。您也可以单击某个IP后的**删除**，单独将其从白名单中移除。
   - 下载白名单
     a. 单击**下载**，下发白名单导出任务。
     b. 在导出任务已下发提示中，单击**确定**。
     c. 关闭**设置黑/白名单**页面，返回上一级页面。
     d. 单击页面右上角的图标，展开任务列表。
     e. 定位到白名单导出任务，等待**任务状态**变为**已完成**，单击**操作**列下的**下载**。

     成功下载白名单IP到本地后，您可以打开下载的TXT文件，查看白名单明细。

# 7.1.2. 设置UDP反射攻击防护

UDP协议流量接入DDoS高防实例进行防护后，推荐您开启UDP反射攻击防护。UDP反射攻击防护支持一键过滤常见的UDP反射攻击，使DDoS高防实例在处理UDP协议流量时，直接丢弃您指定的UDP反射源端口的流量。本文介绍了UDP反射攻击防护的设置方法。

## 前提条件

- 已购买**增强功能**套餐的DDoS高防（新BGP、国际）实例。相关操作，请参见购买DDoS高防实例。

  目前只有增强功能套餐的DDoS高防实例支持设置UDP反射攻击防护。如果您使用的是标准功能套餐实例，则必须升级到增强功能套餐，才能使用UDP反射攻击防护。关于升级实例的具体操作，请参见升级实例。
- 已在**端口接入**页面添加了UDP协议的转发规则。相关操作，请参见添加规则。

UDP反射攻击防护仅对UDP协议流量有效。因此，您只有将UDP协议的业务接入DDoS高防实例进行防护后，才需要设置UDP反射攻击防护。

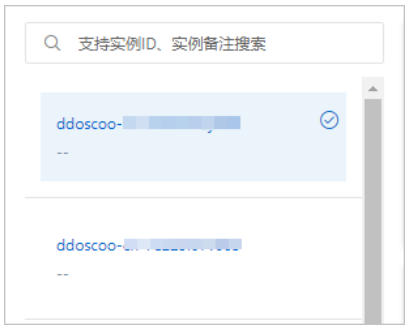
如果您还没有在**端口接入**页面添加任何端口转发规则，或者只添加了TCP协议转发规则，则DDoS默认丢弃所有UDP协议流量。这种情况下，您无需设置UDP反射攻击防护。

## 操作步骤

1. 登录DDoS高防控制台。
2. 在顶部菜单栏左上角处，选择服务所在地域：
   - **中国内地**：选择该地域将跳转到**DDoS高防（新BGP）**控制台。
   - **非中国内地**：选择该地域将跳转到**DDoS高防（国际）**控制台。

     您可以通过切换地域分别管理和配置DDoS高防（新BGP）和DDoS高防（国际）实例。在使用DDoS高防服务时，请确认您已选择正确的地域。
3. 在左侧导航栏，选择**防护设置 > 通用防护策略**。
4. 在**基础设施DDoS防护**页签，从左侧实例列表中选择要设置的DDoS高防实例。

   您可以使用实例ID、实例备注搜索目标实例。




5. 定位到**UDP反射攻击防护（针对高防实例IP）**区域，单击**设置**。

   > **注意** 目前只有增强功能套餐的DDoS高防实例支持设置UDP反射攻击防护。如果您使用的是标准功能套餐实例，可以单击**升级增强版**，将当前实例升级到增强功能套餐，然后才可以设置UDP反射攻击防护。


6. 在**设置UDP反射攻击防护**面板，设置过滤策略（即要过滤的UDP反射源端口）。

   过滤策略表示丢弃指定源端口的UDP协议流量，针对DDoS高防实例生效。如果您在DDoS高防实例上添加了多条UDP业务转发规则，则DDoS高防实例在处理不同UDP业务流量时，都会应用此处设置的过滤策略。


您可以根据业务实际情况，使用以下方式设置过滤策略：

- **一键过滤策略**（推荐）：从**一键过滤策略**区域的策略列表，选中要应用的策略。

  策略列表罗列了常见的UDP反射攻击类型，以及被用于发动对应反射攻击的反射源端口。建议您全选策略列表中的端口，对常见的UDP反射攻击源端口都开启过滤策略。

- **自定义过滤策略**：在**自定义过滤策略**区域在的**反射源端口列表**框，输入要过滤的其他UDP反射源端口（范围：0~65535）。最多支持设置20个端口，多个端口间使用英文逗号（,）分隔。

  该方式适用于过滤一键过滤策略列表中未涵盖的端口，不支持添加与一键过滤策略列表中相同的端口。

7. 单击**确定**。
   设置成功后，DDoS高防实例在处理UDP协议流量时，将直接丢弃被过滤的源端口的UDP协议流量，避免业务遭受UDP反射攻击。您可以根据业务实际需要，在DDoS高防控制台修改UDP反射攻击防护的过滤策略。

# 7.1.3. 设置近源流量压制

近源流量压制指对DDoS高防实例中的电信、联通线路的海外流量实行主动封禁。每个用户总共拥有10次触发流量封禁的额度，且在流量封禁期间支持随时解除封禁。

## 前提条件

已开通DDoS高防（新BGP）实例。相关操作，请参见购买DDoS高防实例。

> **说明** 目前仅DDoS高防（新BGP）服务支持近源流量压制功能。如果您使用DDoS高防（国际）服务，则暂时无法使用该功能。

## 背景信息

当您的DDoS高防实例遭遇特大流量攻击，且发现攻击流量有超过实例最大防护能力的趋势时，建议您考虑使用近源流量压制。一般情况下，假如海外攻击流量占比30%左右，通过封禁海外流量即可大大缓解防御压力，将攻击规模控制在实例最大防护能力范围内。

开启近源流量压制会将特定流量在机房侧丢弃，降低DDoS高防电信、联通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，开启流量封禁可在一定情况下降低被黑洞的概率。

## 操作步骤

1. 登录DDoS高防控制台。
2. 在顶部导航栏，选择**中国内地**地域。
3. 在左侧导航栏，选择**防护设置 > 通用防护策略**。
4. 在**基础设施DDoS防护**页签下，从左侧实例列表中选择要设置的DDoS高防实例。

   > **说明** 您可以使用实例ID、实例备注搜索目标实例。

5. 定位到**近源流量压制**配置区域，根据需要执行以下封禁操作：

   - 封禁电信海外流量：单击**电信海外**后的**操作**，并在**流量封禁**对话框中设置**封禁时长**，完成后单击**确定**。

     > **说明** 每次封禁时长最短15分钟，最长23小时59分钟。

   - 封禁联通海外流量：单击**联通海外**后的**操作**，并在**流量封禁**对话框中设置**封禁时长**，完成后单击**确定**。

     > **说明** 每次封禁时长最短15分钟，最长23小时59分钟。

     > **说明**
     > - 建议您优先封禁电信海外流量，并观察攻击规模的变化趋势。如果攻击流量还是很大，超过当前防护能力，则可以考虑再封禁联通海外流量。
     > - 一个阿里云账号总共拥有10次封禁机会，封禁次数不会每天刷新。封禁一次电信或联通海外流量都会消耗一次额度。

   如果近源流量压制失败，您会收到失败提示信息，请根据提示排查问题后再次尝试。如果未出现任何提示信息，则表示近源流量压制已成功。

6. （可选）回到**近源流量压制**配置区域，单击**查看封禁信息**，在**近源流量封禁**面板查看本次封禁的区域

和时间范围。


7. （可选）解除封禁。

   流量封禁期间，您可以单击**解封**，提前解除对应线路的海外流量封禁。

# 7.1.4. 设置区域封禁

区域封禁指针对访问DDoS高防实例的源IP，按地理区域在清洗机房进行一键封禁，帮助您一键阻断来自指定地区的源IP的访问请求。该功能针对增强功能套餐的DDoS高防实例生效。开启区域封禁后，由封禁地区到DDoS高防实例的流量将被丢弃。本文介绍了设置和开启区域封禁的操作方法。

## 前提条件

已开通增强功能套餐的DDoS高防实例。更多信息，请参见购买DDoS高防实例。

## 背景信息

区域封禁通过直接丢弃来自指定中国地区、海外地区和国家来源IP的所有访问请求，达到阻断非业务来源请求的目的。假设访问DDoS高防实例的正常用户均来自中国，您可以为DDoS高防实例设置区域封禁，封禁来自海外地区或国家的访问请求。

> **说明** 区域封禁针对DDoS高防实例生效。如果您需要对多个不同DDoS高防实例开启区域封禁，则需要对不同DDoS高防实例分别进行设置。不支持对多个DDoS高防实例批量设置。

### 区域封禁VS近源流量压制

区域封禁在DDoS高防清洗机房内部实现，在靠近被攻击目标的位置丢弃特定区域的流量（近目的流量封禁）。区域封禁根据源IP的归属区域在DDoS高防中识别过滤，并不能减小进入高防网络的攻击流量，适用于防护连接资源消耗型攻击。

相比于区域封禁，近源流量压制一般通过运营商骨干网核心路由器，在靠近攻击源的位置丢弃特定区域的流量（例如海外流量）。更多信息，请参见设置近源流量压制。

> **说明** 目前仅DDoS高防（新BGP）服务支持近源流量压制功能。

### 区域封禁VS针对域名的区域封禁

针对域名的区域封禁功能和（针对DDoS高防实例的）区域封禁功能一起使用时，后者优先生效。

例如，针对DDoS高防实例已经通过区域封禁功能封禁了海外地区的流量，关联该DDoS高防实例的域名无论有没有设置区域封禁（针对域名）功能，海外地区用户都不能访问。如果需要实现部分业务封禁海外地区访问，部分业务不封禁海外地区访问，建议您设置针对域名的区域封禁，而非针对DDoS高防实例设置区域封禁。更多信息，请参见设置区域封禁（针对域名）。

## 操作步骤

1. 登录DDoS高防控制台。

2. 在顶部菜单栏左上角处，选择服务所在地域：
   - **中国内地**：选择该地域将跳转到**DDoS高防（新BGP）**控制台。
   - **非中国内地**：选择该地域将跳转到**DDoS高防（国际）**控制台。

     您可以通过切换地域分别管理和配置DDoS高防（新BGP）和DDoS高防（国际）实例。在使用DDoS高防服务时，请确认您已选择正确的地域。
3. 在左侧导航栏，选择**防护设置 > 通用防护策略**。
4. 在**基础设施DDoS防护**页签下，从左侧实例列表中选择要设置的DDoS高防实例。

   > **说明** 您可以使用实例ID、实例备注搜索目标实例。

5. 定位到**区域封禁**配置区域，单击**设置**。
6. 在**封禁区域设置**页面，勾选要封禁的访问请求的来源地区，并单击**确定**。
7. 回到**区域封禁**配置区域，开启区域封禁的**状态**开关，为DDoS高防实例应用区域封禁设置。

# 7.1.5. 黑洞解封

对于已接入DDoS高防的业务，如果因为其保底防护带宽或弹性防护带宽不足被突发大流量攻击造成黑洞，您可以在DDoS高防控制台使用黑洞解封来快速恢复业务。建议您在解除黑洞前先提升保底或弹性防护能力，避免解封后DDoS高防实例再次被攻击到进入黑洞状态。

## 前提条件

已开通DDoS高防（新BGP）实例。

> **说明** 目前仅DDoS高防（新BGP）服务支持黑洞解封功能；DDoS高防（国际）暂不支持黑洞解封。

## 背景信息

每个阿里云账号每天有5次黑洞解封的机会，每天零点自动恢复为5次。

只有成功解除黑洞状态才会消耗一次解封机会。当天第一次解封一般可以即刻解除黑洞状态，如果同一天内连续使用黑洞解封，则相邻两次解封操作的间隔必须大于10分钟。

## 操作步骤

1. 登录DDoS高防控制台。
2. 在顶部导航栏，选择**中国内地**地域。

   您可以通过切换地域分别管理和配置DDoS高防（新BGP）和DDoS高防（国际）实例。在使用DDoS高防服务时，请确认您已选择正确的地域。
3. 在左侧导航栏，选择**防护设置 > 通用防护策略**。
4. 在**基础设施DDoS防护**页签下，从左侧实例列表中选择需要解封的DDoS高防实例。

   您可以使用实例ID、实例备注搜索目标实例。
5. 定位到**黑洞解封**配置区域，根据当前实例状态，执行黑洞解封。


- 如果实例处于**黑洞**状态，且您不希望等待黑洞自动解封，您可以单击**解封**，耐心等待黑洞状态成功解除。
- 如果实例是**正常**状态，则**解封**按钮不可操作。

  相邻两次解封操作的间隔时间必须大于10分钟。

### 执行结果

- 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。
- 如果系统提示“受机房风控影响，暂时无法解封，请10分钟后再尝试”，则请您耐心等待后再尝试。
- 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DDoS高防线路是否已恢复正常。

### 相关文档

- ModifyBlackholeStatus

# 7.1.6. 连接已被黑洞的服务器

本文介绍了在服务器进入黑洞时，通过阿里云同地域ECS服务器连接被黑洞服务器的方法。

### 背景信息

假如您的服务器遭受大流量攻击而进入黑洞，则所有来自外部的流量都会被丢弃，但是阿里云内部与该服务器同地域的云产品仍然能够正常连通该服务器。

因此，在您的服务器进入黑洞后，您可以使用阿里云内部的ECS云服务器连接该服务器。

### 操作步骤

1. 登录与被黑洞服务器同地域且可正常访问的ECS云服务器。

   > **说明** 该ECS云服务器需要与被黑洞的服务器可连通，属于同一个专有网络VPC环境，且连接不被安全组的相关访问控制规则所阻断。更多信息，请参见安全组概述。

2. 在ECS云服务器中，通过工具或命令连接黑洞状态的服务器。
   通过ECS云服务器成功连接该服务器后，您可以将处于黑洞状态的服务器上的文件转移至已登录的ECS云服务器，您也可以通过这种方式变更该服务器上的配置文件等。

# 7.2. 网站业务DDoS防护

# 7.2.1. 设置AI智能防护

DDoS高防为已接入防护的网站业务提供AI智能防护功能。AI智能防护基于阿里云的大数据能力，能够自学习网站业务流量基线，结合算法分析攻击异常，并自动下发精确访问控制规则，动态调整业务防护模型，帮助您及时发现并阻断恶意攻击，例如恶意Bot、HTTP Flood攻击。本文介绍了AI智能防护的使用方法。

## 前提条件

已通过DDoS高防域名接入功能配置了要防护的网站业务。更多信息，请参见添加网站。

## 背景信息

网站业务接入DDoS高防后，默认开启AI智能防护策略，让智能分析引擎自学习网站业务流量基线，并结合精确访问控制规则，实现自主防御恶意Web攻击。

## 设置策略

1. 登录DDoS高防控制台。
2. 在顶部菜单栏左上角处，选择服务所在地域：
   - **中国内地**：选择该地域将跳转到**DDoS高防（新BGP）**控制台。
   - **非中国内地**：选择该地域将跳转到**DDoS高防（国际）**控制台。

     您可以通过切换地域分别管理和配置DDoS高防（新BGP）和DDoS高防（国际）实例。在使用DDoS高防服务时，请确认您已选择正确的地域。
3. 在左侧导航栏，选择**防护设置 > 通用防护策略**。
4. 在**通用防护策略**页面，单击**网站业务DDoS防护**页签，并从左侧域名列表中选择要设置的域名。
5. 定位到**AI智能防护**配置区域，单击**设置**。


6. 在**AI智能防护**对话框，选择智能防护的**模式**和**等级**，并开启**状态**开关。


AI智能防护配置说明：

- **模式：预警、防护**

  AI智能防护支持预警和防护两种工作模式。

- **预警**：检测发现恶意请求时，仅记录攻击预警日志，不会阻断任何访问请求，帮助您了解AI智能防护的效果。

  使用预警模式时，您可以结合全量日志分析，查询与AI智能防护有关的攻击预警记录，确认其攻击防护能力。更多信息，请参见查看攻击预警日志。

- **防护**：检测发现恶意请求时，直接下发能够阻断恶意请求的精确访问控制规则，拦截恶意请求。

  > **说明** AI智能防护通过精确访问控制规则触发防护动作，要使防护生效，您必须开启精确访问控制。更多信息，请参见设置精准访问控制。

  一般情况下，建议您先使用预警模式，并通过全量日志分析报表观察攻击日志记录。在完全确认AI智能防护的效果后，再开启防护模式，使AI智能防护真实生效。

- **等级：宽松、正常、严格**

  开启AI智能防护时，您可以根据网站性能和防护需求，选择应用不同的防护等级。AI智能防护提供宽松、正常和严格三种防护等级。

| 防护等级 | 防护效果 | 应用场景 |
| --- | --- | --- |
| **宽松** | 仅拦截已知的特定恶意攻击，不会对正常请求造成误拦截。 | 适合于比较大型的网站且自身处理性能比较强劲的用户，适用于大促等特定场景。 |
| **正常**（推荐） | 一般情况下，不对请求进行任何处置。当检测到流量对网站造成威胁时，对恶意攻击进行智能防御，对网站的正常业务影响极低。 | 适合请求量平稳且服务器处理性能在处理正常流量的基础上尚有冗余的场景。 |
| **严格** | 对恶意攻击进行严格的智能防御，可能存在部分误拦截的现象。 | 适合网站性能较差或防护效果不佳的场景。 |

成功开启AI智能防护后，DDoS高防在检测到恶意攻击行为时，自动生成精确访问控制防护规则。您可以在精确访问控制模块中查看具体防护规则。

## 查看AI智能防护规则

1. 登录DDoS高防控制台。
2. 在顶部菜单栏左上角处，选择服务所在地域：
   - **中国内地**：选择该地域将跳转到**DDoS高防（新BGP）**控制台。
   - **非中国内地**：选择该地域将跳转到**DDoS高防（国际）**控制台。

     您可以通过切换地域分别管理和配置DDoS高防（新BGP）和DDoS高防（国际）实例。在使用DDoS高防服务时，请确认您已选择正确的地域。
3. 在左侧导航栏，选择**防护设置 > 通用防护策略**。
4. 在**通用防护策略**页面，单击**网站业务DDoS防护**页签，并从左侧域名列表中选择要设置的域名。
5. 定位到**精确访问控制**配置区域，单击**设置**。


6. 在**精确访问控制**页面，查看名称以smartcc_ 开头的规则。

   AI智能防护自动生成的精确访问控制规则的名称均以smartcc_开头。与自定义的精确访问控制规则不同，AI智能防护规则具有以下特性：

   - 规则动作可能是预警。在预警模式下，AI智能防护自动生成的精准防护规则的动作均是预警（只记录攻击日志，不进行拦截）。
   - 具有时效性。AI智能防护下发的规则存在有效期，超过有效期，防护规则自动失效并清除。
   - 不支持手动删除。如果您关闭AI智能防护，则所有AI智能防护规则立即清空。

## 查看攻击预警日志

网站业务开启AI智能防护后，当DDoS高防检测到恶意攻击行为且命中AI智能防护的防护规则时，DDoS高防的全量日志分析功能将记录相应的攻击日志。您可以在全量日志分析中查询与AI智能防护的防护规则关联的攻击预警日志，了解AI智能防护的防护效果。

> **注意** 在执行查询操作前，请确认您已为网站域名开启全量日志分析功能。更多信息，请参见快速上手。

查询语句

登录DDoS高防控制台，前往**调查分析 > 全量日志分析**页面，选择域名并输入以下查询语句，查看与AI智能防护相关的攻击预警日志。

> **说明** 请将 `aliyundoc.com` 替换为您的网站域名。

```
matched_host:"aliyundoc.com" and cc_action:alarm
```

## 调整智能AI防护策略

当业务存在如下特殊场景时，建议调整AI智能防护策略，以确保AI策略得到充分学习，防止误拦截。

| 场景 | 优化方法 |
| --- | --- |
| 网站接入DDoS高防前，源站配置了常规限速策略或频繁出现大量客户端同时重连，业务正常情况下返回大量4XX或5XX状态码。 | 1. 在**网站业务DDoS防护**页签，单击**AI智能防护**模块下的**设置**。<br>2. 在**AI智能防护**对话框，将**模式**调整为**预警**。<br>3. 等待3天后，再将**模式**修改为**防护**。 |

| 场景 | 优化方法 |
| --- | --- |
| 业务网站即将进行大促或压测，源站返回大量4XX或5XX状态码。 | 1. 在**防护设置 > 定制场景策略**页面，单击左上角**创建场景策略**。<br>2. 在**创建场景策略**对话框，配置策略名称和生效时间，单击**确定**后完成策略的创建。<br>3. 在场景策略列表页面，定位到目标策略，并单击**操作**列的**配置对象**。<br>4. 在**重保**面板，选择需要防护的网站或IP，将其添加到重保场景策略的防护对象中。 |

# 7.2.2. 设置黑白名单（针对域名）

DDoS高防支持对已接入防护的网站业务设置针对域名的黑白名单。开启黑白名单（针对域名），则黑名单IP/IP段对域名的访问请求会被直接阻断，白名单IP/IP段对域名的访问请求会被直接放行，且不经过任何防护策略过滤。本文介绍了设置针对域名的黑白名单的方法。

## 前提条件

已在DDoS高防域名接入中配置要防护的网站业务。更多信息，请参见添加网站。

## 背景信息

> **注意** DDoS高防控制台在顶部导航栏新增地域切换菜单，方便您切换选择DDoS高防（新BGP）、DDoS高防（国际）服务。地域切换菜单支持**中国内地**和**非中国内地**选项，您可以通过切换地域分别管理和配置DDoS高防（新BGP）和DDoS高防（国际）实例。在使用DDoS高防服务时，请确认您已选择正确的地域。

网站业务接入DDoS高防后，若存在对网站业务访问量较大的恶意IP，您可以将这些IP添加至针对域名的黑名单，拦截其访问请求。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，您可以将这些IP添加至针对域名的白名单予以放行，来自白名单IP的访问请求不会被拦截。

注意事项

- 针对域名的黑白名单仅支持防护网站业务。对于非网站业务若有类似需求，建议您设置基础设施DDoS防护策略下的黑白名单。更多信息，请参见设置黑白名单（针对高防实例IP）。

  > **说明** 目前仅DDoS高防（新BGP）服务支持黑白名单（针对目的IP）功能。

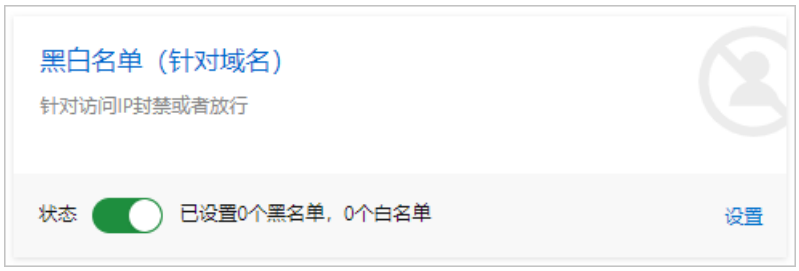
- 黑白名单（针对域名）的设置仅对单个域名生效，而不是对整个DDoS高防实例。
- 针对单个域名，您最多可以分别配置200个黑名单、白名单IP或IP段。

## 操作步骤

1. 登录DDoS高防控制台。
2. 在顶部菜单栏左上角处，选择服务所在地域：
   - **中国内地**：选择该地域将跳转到**DDoS高防（新BGP）**控制台。
   - **非中国内地**：选择该地域将跳转到**DDoS高防（国际）**控制台。

     您可以通过切换地域分别管理和配置DDoS高防（新BGP）和DDoS高防（国际）实例。在使用DDoS高防服务时，请确认您已选择正确的地域。

3. 在左侧导航栏，选择**防护设置 > 通用防护策略**。
4. 在**通用防护策略**页面，单击**网站业务DDoS防护**页签，并从左侧域名列表中选择要设置的域名。
5. 定位到**黑白名单（针对域名）**配置区域，单击**设置**。




6. 在**黑白名单设置**对话框，分别设置黑名单和白名单，并单击**确定**。
   - 选择**黑名单**页签，填写需要拦截其访问请求的恶意IP或IP段。
   - 选择**白名单**页签，填写需要放行其访问请求的正常IP或IP段。

> **说明**
> - IP或IP段支持以IP或IP/掩码的格式填写。
> - 黑名单或白名单下最多均支持添加200个IP或IP段，多个IP或IP段之间用英文逗号（,）分隔。
> - 黑名单支持添加0.0.0.0/0，表示拦截来自除白名单中配置的正常IP外所有IP的访问请求。


7. 回到**黑白名单（针对域名）**配置区域，开启**状态**开关，使黑白名单设置生效。

> **说明** 若您使用旧版本防护设置，则必须开启CC安全防护功能，才能使黑白名单设置生效。

## 执行结果

成功开启针对域名的黑白名单后，黑白名单设置将应用到所有与域名关联的DDoS高防实例，并针对域名的访问流量即刻生效。

> **说明** 在部分情况下，可能需要经过一些访问流量和时间后，黑白名单（针对域名）设置才会真正生效。如果黑白名单（针对域名）开启后，设置未立即生效，请尝试继续访问域名数次。

# 7.2.3. 设置区域封禁（针对域名）

DDoS高防支持对已接入防护的网站业务设置基于地理区域的访问请求封禁策略。开启针对域名的区域封禁功能后，您可以一键阻断指定地区来源IP对网站业务的所有访问请求。本文介绍了设置针对域名的区域封禁的方法。

## 前提条件

- 已在DDoS高防域名接入中配置要防护的网站业务，且关联了增强功能套餐的DDoS高防实例。更多信息，请参见添加网站。
- 已开启新版防护设置。

## 背景信息

网站业务接入DDoS高防后，假设网站的正常用户均来自中国，则您可以开启区域封禁（针对域名），封禁来自非中国地区的访问请求。同理，您可以设置封禁其他非正常网站用户来源的区域。设置区域封禁（针对域名）时，您只需选择要封禁的区域即可。

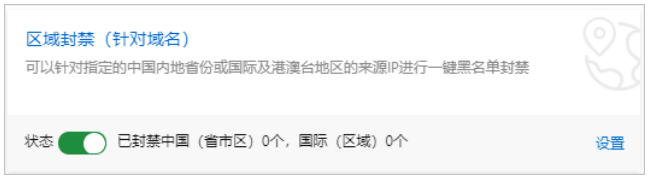
注意事项

- 区域封禁（针对域名）仅支持防护网站业务。对于非网站业务若有类似需求，建议您设置基础设施DDoS防护策略下的流量封禁。更多信息，请参见设置近源流量压制（目前仅新BGP高防支持）、设置区域封禁。
- 区域封禁（针对域名）对域名生效。如果您需要为多个域名设置区域封禁，则需要为不同域名分别设置，不支持对多个域名批量设置区域封禁。
- 区域封禁（针对域名）根据源IP的归属区域在DDoS高防中识别过滤，并不能减小进入高防网络的攻击流量。

## 操作步骤

1. 登录DDoS高防控制台。
2. 在顶部菜单栏左上角处，选择服务所在地域：
   - **中国内地**：选择该地域将跳转到**DDoS高防（新BGP）**控制台。
   - **非中国内地**：选择该地域将跳转到**DDoS高防（国际）**控制台。

     您可以通过切换地域分别管理和配置DDoS高防（新BGP）和DDoS高防（国际）实例。在使用DDoS高防服务时，请确认您已选择正确的地域。
3. 在左侧导航栏，选择**防护设置 > 通用防护策略**。
4. 在**通用防护策略**页面，单击**网站业务DDoS防护**页签，并从左侧域名列表中选择要设置的域名。
5. 定位到**区域封禁（针对域名）**区域，单击**设置**。




6. 在**封禁区域设置**页面，选中要封禁的**中国（省市区）**或**国际（区域）**，并单击**确定**。

7. 回到**区域封禁（针对域名）**区域，开启**状态**开关，应用针对域名的区域封禁设置。

## 执行结果

成功开启针对域名的区域封禁后，区域封禁设置将应用到所有与域名关联的DDoS高防实例，并针对域名的访问流量即刻生效。

# 7.2.4. 设置精准访问控制

DDoS高防支持对已接入防护的网站业务设置精准访问控制策略。开启精确访问控制后，您可以使用常见的HTTP字段（例如IP、URL、Referer、UA、参数等）设置匹配条件来筛选访问请求，并对命中条件的请求设置放行、封禁、挑战操作。精准访问控制支持业务场景定制化的防护策略，可用于盗链防护、网站管理后台保护等场景。

## 前提条件

- 已在DDoS高防域名接入中配置要防护的网站业务。更多信息，请参见添加网站。
- 已开启新版防护设置。

## 背景信息

网站业务接入DDoS高防后，如果您需要针对性地管理具有固定特征的访问请求，则您可以为域名开启精确访问控制并设置精确访问控制规则。精准访问控制规则由匹配条件与匹配动作构成。

- 匹配条件定义了要识别的请求特征，具体指访问请求中HTTP字段的属性特征。精确访问控制规则支持匹配的HTTP字段如下表所示。

> **说明** 不同字段适用的匹配逻辑不同，例如请求源IP字段“属于、不属于”具体的值，请求URI“包括、不包括”具体的内容等，详见下表中“适用的逻辑符”一列。

| 匹配字段 | 字段描述 | 适用的逻辑符 |
| --- | --- | --- |
| IP | 访问请求的来源IP。 | 属于、不属于 |
| URI | 访问请求的URI地址。 | 包括、不包括 、等于、不等于、长度小于、长度等于、长度大于 |
| User-Agent | 发起访问请求的客户端浏览器标识等相关信息。 | 包括、不包括 、等于、不等于、长度小于、长度等于、长度大于 |
| Cookie | 访问请求中的携带的Cookie信息。 | 包括、不包括 、等于、不等于、长度小于、长度等于、长度大于、不存在 |
| Referer | 访问请求的来源网址，即该访问请求是从哪个页面跳转产生的。 | 包括、不包括 、等于、不等于、长度小于、长度等于、长度大于、不存在 |
| Content-Type | 访问请求指定的响应HTTP内容类型，即MIME类型信息。 | 包括、不包括 、等于、不等于、长度小于、长度等于、长度大于 |
| X-Forwarded-For | 访问请求的客户端真实IP。 | 包括、不包括 、等于、不等于、长度小于、长度等于、长度大于、不存在 |
| Content-Length | 访问请求的所包含的字节数。 | 值小于、值等于、值大于 |

| 匹配字段 | 字段描述 | 适用的逻辑符 |
| --- | --- | --- |
| Post-Body | 访问请求的内容信息。 | 包含、不包含、等于、不等于 |
| Http-Method | 访问请求的方法，具体包括GET、POST、DELETE、PUT、OPTIONS、CONNECT、HEAD、TRACE。 | 等于、不等于 |
| Header | 访问请求的头部信息，用于自定义HTTP头部字段及匹配内容。 | 包括、不包括 、等于、不等于、长度小于、长度等于、长度大于、不存在 |
| Params | 访问请求的URL地址中的参数部分，通常指URL中 `?` 后面的部分。例如，`www.abc.com/index.html?action=login` 中的 `action=login` 就是参数部分。 | 包括、不包括 、等于、不等于、长度小于、长度等于、长度大于 |

- 匹配动作定义了访问请求命中匹配条件时，对访问请求执行的动作，具体包括放行、封禁、挑战（通过挑战算法对请求的源IP地址发起校验）。

## 使用限制

根据网站业务关联的DDoS高防实例的功能套餐类型，精确访问控制规则具有如下使用限制。

| 限制 | 标准功能套餐实例 | 增强功能套餐实例 |
| --- | --- | --- |
| 自定义规则数量 | 不超过五条 | 不超过十条 |
| 可使用的匹配字段 | IP、URL、Referer、User-Agent | 所有支持匹配的字段 |

## 操作步骤

1. 登录DDoS高防控制台。
2. 在顶部菜单栏左上角处，选择服务所在地域：
   - **中国内地**：选择该地域将跳转到**DDoS高防（新BGP）**控制台。
   - **非中国内地**：选择该地域将跳转到**DDoS高防（国际）**控制台。

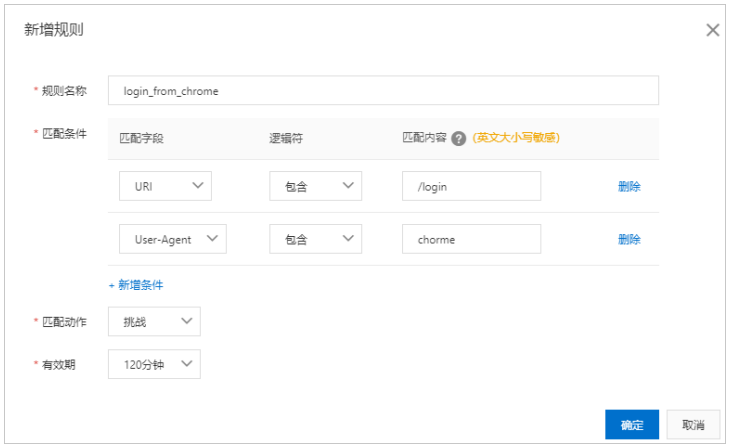
     您可以通过切换地域分别管理和配置DDoS高防（新BGP）和DDoS高防（国际）实例。在使用DDoS高防服务时，请确认您已选择正确的地域。
3. 在左侧导航栏，选择**防护设置 > 通用防护策略**。
4. 在**通用防护策略**页面，单击**网站业务DDoS防护**页签，并从左侧域名列表中选择要设置的域名。
5. 定位到**精确访问控制**配置区域，单击**设置**。

6. 为域名设置精确访问控制规则。


- 新增规则
  a. 单击**新增规则**。

> **说明** 若自定义规则数量达到限制，则**新增规则**不可操作。

  b. 在**新增规则**对话框，完成规则配置，并单击**确定**。




| 参数 | 描述 |
| --- | --- |
| **规则名称** | 规则的名称，由英文字母、数字和下划线（_）组成，不超过128个字符。 |
| **匹配条件** | 规则的匹配条件。单击**新增条件**添加一个条件，每个条件由**匹配字段**、**逻辑符**和**匹配内容**组成。<br>■ 关于匹配字段和逻辑符的取值范围，请参见支持的匹配字段。<br>■ 匹配内容根据匹配字段填写，大小写敏感。暂时不支持通过正则表达式描述，但允许设置为空值。<br>支持添加多个匹配条件。若添加多个匹配条件，则只有当访问请求满足所有条件时才算命中。 |

| 参数 | 描述 |
| --- | --- |
| **匹配动作** | 当访问请求命中匹配条件时，对请求执行的操作。取值：<br>■ **封禁**：阻断命中匹配条件的访问请求。<br>■ **放行**：放行命中匹配条件的访问请求。<br>■ **挑战**：通过挑战算法对命中匹配条件的访问请求的源IP地址发起校验。 |
| **有效期** | 规则的有效期，取值：5分钟、10分钟、30分钟、60分钟、90分钟、120分钟、永久。 |

以上图为例，配置完成后，对于包含 `/login` 页面的请求，如果其UserAgent字段中包含 `chrome` ，则对请求的源IP发起校验。该规则自创建成功起在120分钟内生效。

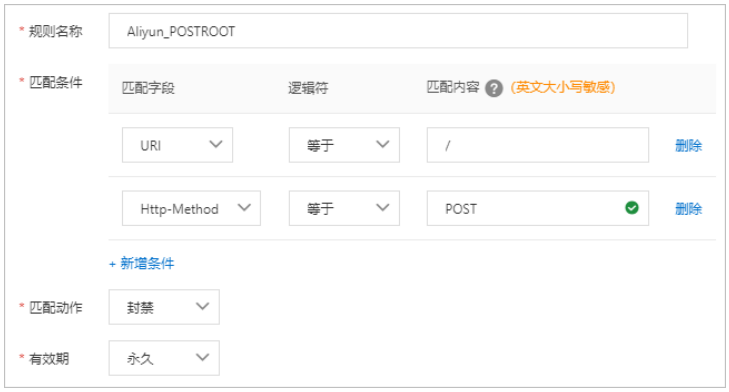
成功添加精确访问控制规则后，您可以根据需要继续添加多条规则。

> **说明**
>
> ■ 如果您设置了多条规则，则规则的优先级遵循其在规则列表中的排列顺序，排序越靠前，优先级越高。访问请求根据规则顺序依次进行匹配，顺序较前的精准访问控制规则优先匹配。
>
> ■ 如果一个请求同时命中多个匹配条件，则匹配动作取所有命中的规则中，排序最靠前的访问控制规则中的匹配动作。

规则配置示例

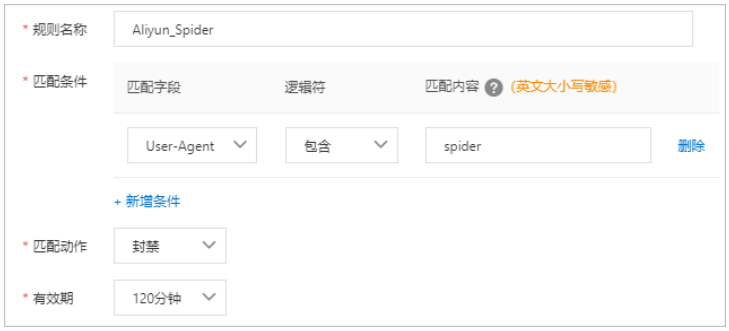
■ 拦截特定的攻击请求：

一般情况下，正常业务不存在POST根目录的请求信息。如果网站业务上发生CC攻击，且您发现客户端的请求中存在大量的POST根目录请求，则可以评估请求的合法性。如果确认其为非正常业务请求，可以通过精准访问控制规则，执行拦截动作。规则配置示例如下。



- 拦截一段时间内爬虫的访问请求：

  如果在某段时间内，您发现网站的访问流量中有大量爬虫请求，若不排除是攻击傀儡机模拟爬虫进行CC攻击，则可以对爬虫的请求执行拦截操作。规则配置示例如下。




- 编辑规则
  a. 在规则列表中，定位到要操作的规则，单击其操作列下的**编辑**。
  b. 在**编辑规则**对话框中，修改规则配置，并单击**确定**。规则配置的描述见新增规则，其中，**规则名称**不可修改。
- 删除规则
  a. 在规则列表中，定位到要删除的规则，单击其操作列下的**删除**。
  b. 在删除提示对话框中，单击**确定**。

7. 回到**精确访问控制**功能区域，开启**状态**开关，应用精确访问控制规则。

# 7.2.5. 设置频率控制

DDoS高防为已接入防护的网站业务提供频率控制防护，支持限制源IP的访问频率。频率控制防护开启后自动生效，默认使用正常防护模式，帮助网站防御一般的CC攻击。频率控制防护提供多种防护模式，供您在不同场景下调整使用。您也可以自定义频率控制规则，限制单一源IP在短期内异常频繁地访问某个页面。

## 前提条件

- 已在DDoS高防域名接入中配置要防护的网站业务。更多信息，请参见添加网站。
- 已开启新版防护设置。

## 背景信息

网站业务接入DDoS高防后，您可以为网站开启频率控制防护，防御HTTP Flood攻击（即CC攻击）。频率控制防护提供不同的防护模式，允许您根据网站的实时流量异常调整频率控制策略，具体包括以下模式。

- 正常（默认）：网站无明显流量异常时建议采用此模式。正常模式的频率控制防护策略相对宽松，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：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。攻击紧急模式的频率控制防护策略相对严格。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：严格模式的频率控制防护策略较为严格。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，只有通过认证的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：超级严格模式的频率控制防护策略非常严格。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，只有通过认证的访问者才允许访问网站。 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。

除了不同防护模式外，频率控制防护还支持通过自定义防护规则进行更精确的CC攻击拦截。您可以为需要重点保护的URL自定义频率控制策略，限制单一源IP在短期内异常频繁地访问某个页面。

## 设置频率控制防护模式

1. 登录DDoS高防控制台。
2. 在顶部菜单栏左上角处，选择服务所在地域：
   - **中国内地**：选择该地域将跳转到**DDoS高防（新BGP）**控制台。
   - **非中国内地**：选择该地域将跳转到**DDoS高防（国际）**控制台。

     您可以通过切换地域分别管理和配置DDoS高防（新BGP）和DDoS高防（国际）实例。在使用DDoS高防服务时，请确认您已选择正确的地域。
3. 在左侧导航栏，选择**防护设置 > 通用防护策略**。
4. 在**通用防护策略**页面，单击**网站业务DDoS防护**页签，并从左侧域名列表中选择要设置的域名。
5. 定位到**频率控制**配置区域，选择要应用的**内置模式（正常、攻击紧急、严格、超级严格）**，并开启**状态**开关，应用频率控制防护。


## 自定义频率控制防护规则

1. 登录DDoS高防控制台。
2. 在顶部菜单栏左上角处，选择服务所在地域：
   - **中国内地**：选择该地域将跳转到**DDoS高防（新BGP）**控制台。
   - **非中国内地**：选择该地域将跳转到**DDoS高防（国际）**控制台。

     您可以通过切换地域分别管理和配置DDoS高防（新BGP）和DDoS高防（国际）实例。在使用DDoS高防服务时，请确认您已选择正确的地域。

3. 在左侧导航栏，选择**防护设置 > 通用防护策略**。
4. 在**通用防护策略**页面，单击**网站业务DDoS防护**页签，并从左侧域名列表中选择要设置的域名。
5. 定位到**频率控制**配置区域，开启**自定义规则**开关，并单击**设置**。


6. 为域名设置频率控制防护规则。


- 新增规则
  a. 单击**新增规则**。

  > **说明** 最多支持自定义20条规则。若规则数量达到限制，则**新增规则**不可操作。

  b. 在**新增规则**对话框，完成规则配置，并单击**确定**。


| 参数 | 说明 |
| --- | --- |
| **规则名称** | 为该规则命名。 |
| **URI** | 指定需要防护的具体地址，如*/register*。支持在地址中包含参数，如*/user?action=login*。 |
| **匹配规则** | ■ **完全匹配**：即精确匹配，请求地址必须与配置的URI完全一样才会被统计。<br>■ **前缀匹配**：即包含匹配，只要是请求的URI以此处配置的URI开头就会被统计。例如，如果设置URI为*/register*，则*/register.html*会被统计。 |
| **检测时长** | 指定统计访问次数的周期。需要和单一IP访问次数配合。 |
| **单一IP访问次数** | 指定在检测时长内，允许单个源IP访问被防护地址的次数。 |
| **阻断类型** | 指定触发条件后的操作（封禁、人机识别），以及请求被阻断后阻断动作的时长。<br>■ **封禁**：触发条件后，直接断开连接。<br>■ **人机识别**：触发条件后，用重定向的方式去访问客户端（返回200状态码），通过验证后才放行。例如，单个IP在20s内访问超过5次则进行人机识别判断，在10分钟内该IP的访问请求都需要通过人机识别，如果被识别为非法将会被拦截，只有被识别为合法才会放行。 |

成功添加频率控制自定义规则后，您可以根据需要继续添加多条规则。

- 编辑规则

  a. 在规则列表中，定位到要操作的规则，单击其操作列下的**编辑**。

b. 在**编辑规则**对话框中，修改规则配置，并单击**确定**。规则配置的描述见新增规则，其中，**规则名称**和**URI**不可更改。

- 删除规则
  a. 在规则列表中，定位到要删除的规则，单击其操作列下的**删除**。
  b. 在删除提示对话框中，单击**确定**。

7. 回到**频率控制**配置区域，开启**状态**开关，应用频率控制自定义规则。

### 频率控制防护设置最佳实践

频率控制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频率控制防护模式。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。

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，需要通过配置频率控制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。

## 7.2.6. 设置DDoS全局防护策略

DDoS防护引擎根据流量清洗力度，为接入高防防护的网站业务提供三套内置的全局防护策略，帮助业务在攻击发生的瞬间快速应对脉冲式攻击，提高响应及时性。本文介绍了DDoS全局防护策略的设置方法。

### 前提条件

- 已购买DDoS高防（新BGP）实例或DDoS高防（国际）保险版、无忧版、安全加速线路实例。

  相关操作，请参见购买DDoS高防实例。
- 已在**域名接入**页面配置了要防护的网站。

  相关操作，请参见添加网站。

### 背景信息

DDoS全局防护策略包含阿里云DDoS防护引擎在应对常见威胁情报中沉淀的通用防护规则。通过启用全局防护策略，您可以将通用防护规则应用到接入DDoS高防防护的网站业务，减少攻击发生瞬间出现攻击透过的危害。

DDoS全局防护策略支持为每个接入防护的域名单独开启或关闭，并提供**正常**、**宽松**、**严格**三种防护模式。

自2021年11月24日（含）后新接入DDoS高防防护的域名，默认开启了DDoS全局防护策略（**正常**模式）。您可以根据防护需要，修改全局防护策略的模式：

- 需要加强流量清洗力度时（例如，已有策略防护效果不佳的情形），推荐使用**严格**模式。

  > **注意** 使用**严格**模式前，建议您提交工单或通过售后钉钉服务群进行咨询，避免策略调整对业务造成误伤。

- 需要降低流量清洗力度时（例如，业务大促期间），推荐使用**宽松**模式。

> **注意** 如果您在2021年11月24日前已完成域名接入，DDoS全局防护策略默认关闭，建议您手动为域名开启该功能。

### 操作步骤

1. 登录DDoS高防控制台。
2. 在顶部菜单栏左上角处，选择服务所在地域：
   - **中国内地**：选择该地域将跳转到**DDoS高防（新BGP）**控制台。
   - **非中国内地**：选择该地域将跳转到**DDoS高防（国际）**控制台。

     您可以通过切换地域分别管理和配置DDoS高防（新BGP）和DDoS高防（国际）实例。在使用DDoS高防服务时，请确认您已选择正确的地域。
3. 在左侧导航栏，选择**防护设置 > 通用防护策略**。
4. 单击**网站业务DDoS防护**页签，并从左侧域名列表中选择要设置的域名。

   域名列表包含所有已接入DDoS高防防护的网站域名。如果您的域名不在域名列表，请先完成域名接入。相关操作，请参见添加网站。
5. 定位到**DDoS全局防护策略**区域，修改相关设置。


您可以修改以下设置：

- **状态**开关：开启或关闭DDoS全局防护策略功能。建议保持开启状态。
- 防护模式：支持**宽松**、**正常**、**严格**三种模式，具体说明如下。

| 模式 | 防护效果 | 应用场景 |
| --- | --- | --- |
| **宽松** | 只拦截已知的特定恶意攻击，不会对正常请求造成误拦截。 | 适合网站规模较大且自身处理性能较强劲的业务防护场景。 |
| **正常**（推荐） | 拦截在历史正常业务流量中不存在，但在全网恶意攻击中出现概率高的已知恶意攻击，对网站正常业务影响低。 | 适合请求量平稳、业务属性及用户来源不会有大幅变化的业务防护场景。 |
| **严格** | 对恶意攻击进行严格防御，可能存在部分误拦截。 | 适合网站自身处理性能较差的业务防护场景。 |

# 7.3. 非网站业务DDoS防护

## 7.3.1. 设置四层AI智能防护

DDoS高防实例默认启用智能防护功能，通过算法自主学习接入业务的历史流量，自适应调整四层流量清洗策略，提供符合业务场景的防御效果。业务接入DDoS高防后，将直接获得正常等级的智能防护能力，无需您手动设置。若正常等级的防御效果不够理想，您可以根据实际需求选择更宽松或严格的智能防护等级。

### 前提条件

已开通DDoS高防（新BGP）或DDoS高防（国际）实例。更多信息，请参见购买DDoS高防实例。

## 背景信息

针对网络四层DDoS攻击，DDoS高防智能防护结合历史业务流量和阿里云攻防安全专家的经验，提供宽松、正常、严格三种智能防护等级供您选择。 默认情况下，您所购买的DDoS高防实例自动开启四层AI智能防护，并选用正常防护等级。您可以根据实际情况自由调整智能防护等级。

由于智能防护功能通过算法学习您的历史业务流量，因此业务初次接入DDoS高防进行防护时，系统需要三天左右时间完成对您业务流量的学习和训练，从而达到符合业务场景的防御效果。

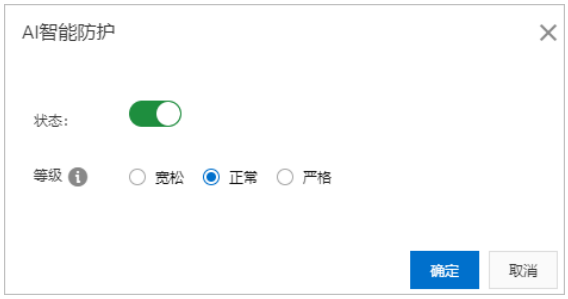
对于带有明显攻击特征的恶意IP，智能防护算法将根据需要自动将其添加到针对DDoS高防实例的流量黑名单中，在一定时间内丢弃其全部访问请求。您可以随时查看或删除黑名单中的IP，也可以在黑名单中手动添加其他恶意IP进行防御。同时，您还可以将特定的IP添加至流量白名单，系统将直接放行来自这些IP的业务访问流量。更多信息，请参见设置黑白名单（针对高防实例IP）。

## 操作步骤

1. 登录DDoS高防控制台。
2. 在顶部菜单栏左上角处，选择服务所在地域：
   - **中国内地**：选择该地域将跳转到**DDoS高防（新BGP）**控制台。
   - **非中国内地**：选择该地域将跳转到**DDoS高防（国际）**控制台。

     您可以通过切换地域分别管理和配置DDoS高防（新BGP）和DDoS高防（国际）实例。在使用DDoS高防服务时，请确认您已选择正确的地域。
3. 在左侧导航栏，选择**防护设置 > 通用防护策略**。
4. 在**通用防护策略**页面，单击**非网站业务DDoS防护**页签，并在页面上方选择要设置的DDoS高防实例。


5. 定位到**AI智能防护**区域，单击**设置**。
6. 在**AI智能防护**对话框，根据攻击情况选择要应用的防护**等级**，并单击**确定**。




不同防护等级的说明如下：

- **宽松**：对来自带有明显攻击特征的恶意IP的流量进行自动清洗。该等级可能无法拦截所有四层流量攻击，但误杀率低。

- **正常**：对来自带有明显攻击特征的恶意IP和疑似恶意IP的流量进行自动清洗。该等级默认启用，能够充分平衡防护效果和误杀率，建议您在一般情况下选择该等级。
- **严格**：对当前正在发生的攻击行为进行严格地防御，但可能存在一定误杀。

成功修改智能防护等级后，目标DDoS高防实例将按照调整后的防护等级工作。

# 7.3.2. 设置DDoS防护策略

DDoS高防提供针对网络四层DDoS攻击的防护策略设置功能，例如虚假源和空连接检测、源限速、目的限速，适用于优化调整非网站业务的DDoS防护策略。在DDoS高防实例下添加端口转发规则，接入非网站业务后，您可以单独设置某个端口的DDoS防护策略或批量添加DDoS防护策略。本文介绍了具体的操作方法。

## 前提条件

已在端口接入中配置非网站业务端口转发规则。更多信息，请参见添加规则。

## 背景信息

> **注意** DDoS高防控制台在顶部导航栏新增地域切换菜单，方便您切换选择DDoS高防（新BGP）、DDoS高防（国际）服务。地域切换菜单支持**中国内地**和**非中国内地**选项，您可以通过切换地域分别管理和配置DDoS高防（新BGP）和DDoS高防（国际）实例。在使用DDoS高防服务时，请确认您已选择正确的地域。

非网站业务的DDoS防护策略是基于“IP地址+端口”级别的防护，对于已接入DDoS高防实例的非网站业务的“IP+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能力。DDoS防护策略配置针对端口级别生效。

DDoS高防为已接入的非网站业务提供以下DDoS防护策略。

- 虚假源：针对虚假IP发起的DDoS攻击进行校验过滤。
- 目的限速：以当前高防IP、端口为统计对象，当每秒访问频率超出阈值时，对当前高防IP的端口进行限速，其余端口不受限速影响。
- 包长度过滤：设置允许通过的包最小和最大长度，小于最小长度或者大于最大长度的包会被丢弃。
- 源限速：以当前高防IP、端口为统计对象，对访问频率超出阈值的源IP地址进行限速。访问速率未超出阈值的源IP地址，访问不受影响。源限速支持黑名单控制，对于60秒内5次超限的源IP，您可以开启将源IP加入黑名单的策略，并设置黑名单的有效时长。

## 设置端口DDoS防护策略

以下步骤描述了单独设置高防IP下某一条转发规则的DDoS防护策略的方法，您也可以在高防IP下批量添加DDoS防护策略，具体请参见批量添加DDoS防护策略。

1. 登录DDoS高防控制台。
2. 在顶部菜单栏左上角处，选择服务所在地域：
   - **中国内地**：选择该地域将跳转到**DDoS高防（新BGP）**控制台。
   - **非中国内地**：选择该地域将跳转到**DDoS高防（国际）**控制台。

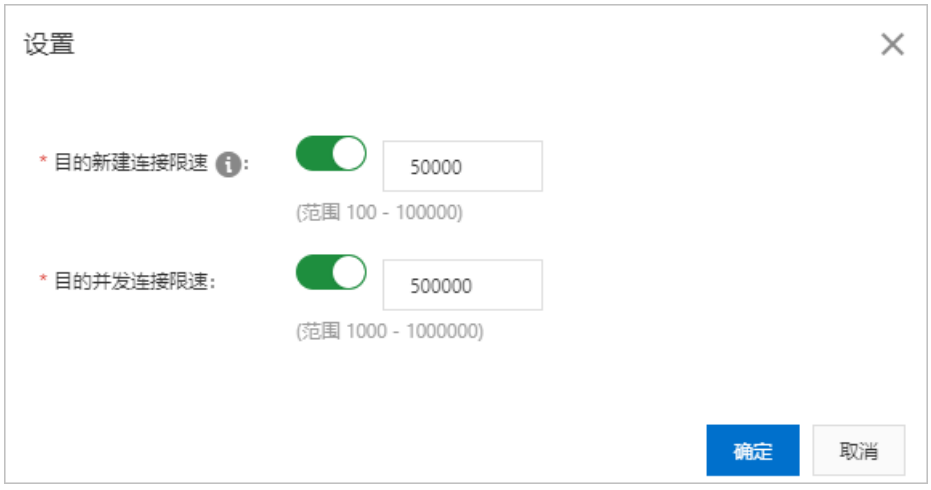
     您可以通过切换地域分别管理和配置DDoS高防（新BGP）和DDoS高防（国际）实例。在使用DDoS高防服务时，请确认您已选择正确的地域。
3. 在左侧导航栏，选择**防护设置 > 通用防护策略**。
4. 在**通用防护策略**页面，单击**非网站业务DDoS防护**页签，并在页面上方选择要设置的DDoS高防实例。

5. 从左侧转发规则列表中单击要设置的转发规则。


6. 为指定的转发规则设置**虚假源**、**目的限速**、**包长度过滤**、**源限速**。
   - **虚假源**：在**虚假源**下开启或关闭**虚假源**和**空连接**开关。

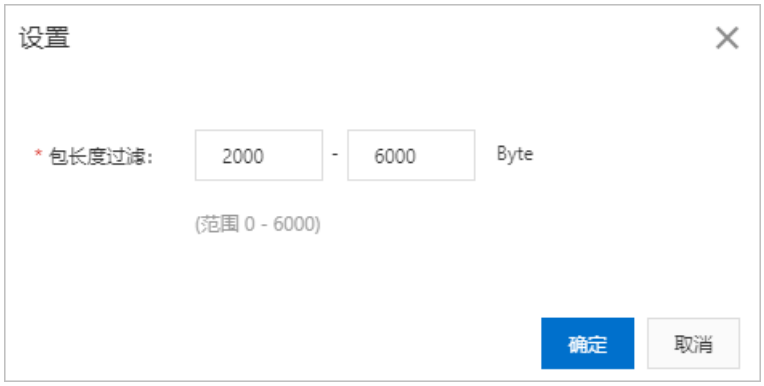
| 参数 | 描述 |
| --- | --- |
| **虚假源** | 虚假源地址攻击防护开关。开启后将自动过滤虚假源IP地址的连接请求。<br>**说明** 仅适用于TCP协议规则。 |
| **空连接** | 空连接防护开关。开启后将自动过滤空连接请求。<br>**说明** 仅适用于TCP协议规则，且要开启空连接，必须先开启虚假源。 |

   - **目的限速**：单击**目的限速**下的**设置**，在**设置**对话框完成以下配置，并单击**确定**。



| 参数 | 描述 |
| --- | --- |
| **目的新建连接限速** | 限制高防IP端口每秒最大新建连接数，取值范围：100~100000（个）。超过限制的新建连接将被丢弃。<br>**说明** 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** | 限制高防IP端口的最大并发连接数量，取值范围：1000~1000000（个）。超过限制的并发连接将被丢弃。 |

- **包长度过滤**：单击**包长度过滤**下的**设置**，在**设置**对话框设置允许通过高防IP端口的报文所含payload的最小和最大长度，取值范围：0~6000（Byte），并单击**确定**。




- **源限速**：单击**源限速**下的**设置**，在**源限速设置**页面完成以下配置，并单击**确定**。


源限速设置
* 源新建连接限速 :
自动
手动
关闭
* 源并发连接限速:
每秒单个源并发连接达到
1
个，做限速处理
(范围 1- 50000)
源并发连接60秒内5次超限，将该源IP加入黑名单
黑名单有效时长
30
分钟
(范围 1 - 10080)
* 源PPS限速
当源PPS达到
1
Packet/s，做限速处理
(范围 1 - 100000)
源PPS连接60秒内5次超限，将该源IP加入黑名单
黑名单有效时长
30
分钟
(范围 1 - 10080)
* 源带宽限速
当源带宽达到
1024
Byte/s，做限速处理
(范围 1024 - 268435456)
源带宽连接60秒内5次超限，将该源IP加入黑名单
黑名单有效时长
30
分钟
(范围 1 - 10080)
确定
取消

| 参数 | 描述 |
| --- | --- |

| 参数 | 描述 |
| --- | --- |
| **源新建连接限速** | 限制单一源IP的每秒新建连接数量，取值范围：1~50000（个）。超过限制的新建连接将被丢弃。支持**自动**和**手动**模式。<br>■ 启用自动防护模式后，系统将动态自动计算源新建连接限速阈值，无需手动设置。<br>■ 如果选择手动模式，则需要手动设置源新建连接限速阈值。<br>**说明** 由于防护设备为集群化部署，新建连接限速存在一定误差。<br>黑名单策略<br>■ 支持**源新建连接60秒内5次超限，将该源IP加入黑名单**选项，源IP若进入黑名单，则其连接请求都将被丢弃。<br>■ 开启黑名单策略时，需要设置**黑名单有效时长**，取值范围：1~10080（分钟），默认为30分钟。源IP被加入黑名单时，经有效时长后自动被释放。 |
| **源并发连接限速** | 限制单一源IP的并发连接数量，取值范围：1~50000（个）。超过限制的并发连接将被丢弃。<br>黑名单策略<br>■ 支持**源并发连接60秒内5次超限，将该源IP加入黑名单**选项，源IP若进入黑名单，则其连接请求都将被丢弃。<br>■ 开启黑名单策略时，需要设置**黑名单有效时长**，取值范围：1~10080（分钟），默认为30分钟。源IP被加入黑名单时，经有效时长后自动被释放。 |
| **源PPS限速** | 限制单一源IP的包转发数量，取值范围：1~100000（Packet/s）。超过限制的数据包将被丢弃。<br>黑名单策略<br>■ 支持**源PPS连接60秒内5次超限，将该源IP加入黑名单**选项，源IP若进入黑名单，则其连接请求都将被丢弃。<br>■ 开启黑名单策略时，需要设置**黑名单有效时长**，取值范围：1~10080（分钟），默认为30分钟。源IP被加入黑名单时，经有效时长后自动被释放。 |
| **源带宽限速** | 限制单一源IP的源请求带宽，取值范围：1024~268435456（Byte/s）。<br>黑名单策略<br>■ 支持**源带宽连接60秒内5次超限，将该源IP加入黑名单**选项，源IP若进入黑名单，则其连接请求都将被丢弃。<br>■ 开启黑名单策略时，需要设置**黑名单有效时长**，取值范围：1~10080（分钟），默认为30分钟。源IP被加入黑名单时，经有效时长后自动被释放。 |

## 批量添加DDoS防护策略

1. 登录DDoS高防控制台。
2. 在顶部菜单栏左上角处，选择服务所在地域：
   - **中国内地**：选择该地域将跳转到**DDoS高防（新BGP）**控制台。
   - **非中国内地**：选择该地域将跳转到**DDoS高防（国际）**控制台。

     您可以通过切换地域分别管理和配置DDoS高防（新BGP）和DDoS高防（国际）实例。在使用DDoS高防服务时，请确认您已选择正确的地域。
3. 在左侧导航栏，选择**接入管理 > 端口接入**。
4. 在**端口接入**页面，选择DDoS高防实例，并单击规则列表下方的**批量操作 > DDoS防护策略配置**。


5. 在**批量添加DDoS防护策略**对话框，按照格式要求输入要添加的防护策略内容，并单击**添加**。


DDoS防护策略的格式要求如下。

> **说明** 您也可以先批量导出当前DDoS防护策略，在导出的txt文件中统一调整后再将内容复制粘贴进来。导出文件中的DDoS防护策略格式和批量添加DDoS防护策略的格式要求一致。更多信息，请参见批量导出。

- 每行对应一条转发规则的DDoS防护策略。
- 每条DDoS防护策略从左到右包含以下字段：转发协议端口、转发协议（tcp、udp）、源新建连接限速、源并发连接限速、目的新建连接限速、目的并发连接限速、包长度最小值、包长度最大值、虚假源开关、空连接开关（字段的含义和取值范围见DDoS防护策略配置项说明）。字段间以空格分隔。

- 转发协议端口必须是已配置转发规则的端口。
- 虚假源开关和空连接开关的取值是：on、off。若为空则表示关闭（即off）。

# 7.3.3. 设置源限速

源限速允许您对源IP到DDoS高防实例端口的访问频率和流量大小进行限制。开启源限速后，超出访问限制的源IP将触发请求限速或加入黑名单处理。源IP一旦被添加到黑名单，则所有来自该IP的访问请求会被丢弃。本文介绍了设置源限速的具体操作。

## 前提条件

已在端口接入中配置非网站业务端口转发规则。更多信息，请参见添加规则。

## 背景信息

DDoS高防支持对源IP到特定DDoS高防实例端口的访问频率进行限制，限制维度包括源新建和并发连接等，也支持对源IP到特定DDoS高防实例端口的流量大小进行限制，限制维度包括源带宽（bps）和源报文数量（pps）。针对超过访问频率或流量阈值的源IP，DDoS高防对其进行限速和设置黑名单处理。上述功能适用于防护四层连接型CC攻击，能够起到快速压制攻击源的目的，效果明显。

假设某个源IP访问DDoS高防实例的8000端口，新建连接异常高，超出正常水平十多倍。您可以为高防实例的8000端口配置源新建连接限速，且开启黑名单策略，将反复超限的源IP自动添加成黑名单，丢弃源IP的访问请求。

> **说明** 源限速针对DDoS高防实例的具体端口生效。如果您需要对多个不同DDoS高防实例的端口开启源限速，则需要对不同DDoS高防实例的端口分别设置。

## 操作步骤

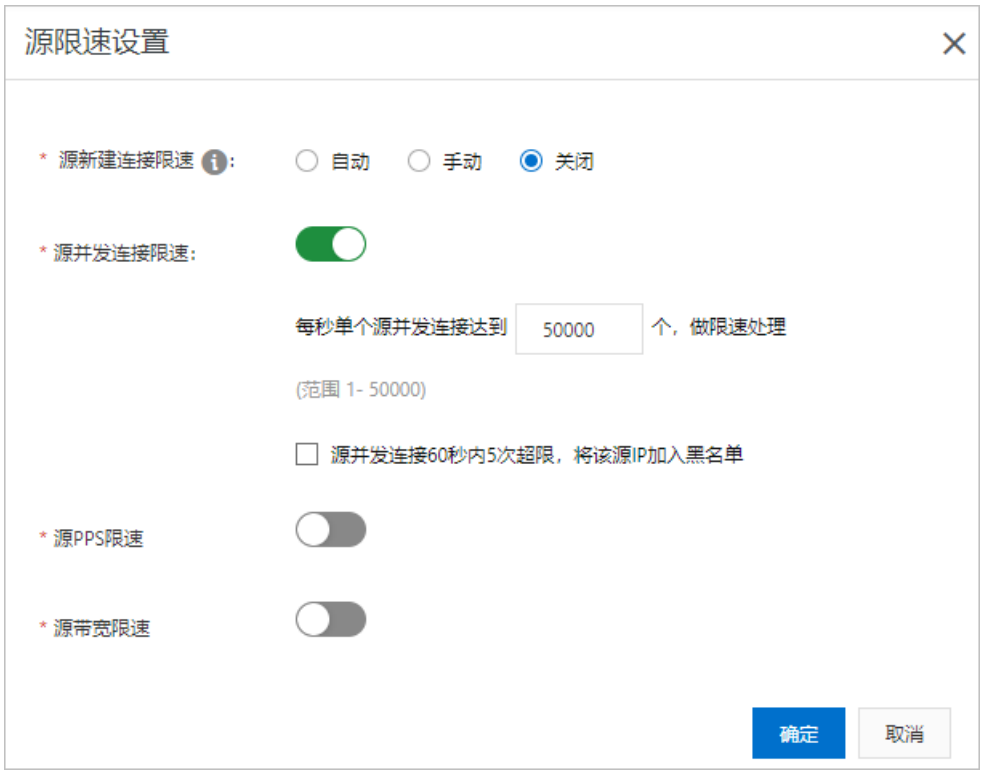
1. 登录DDoS高防控制台。
2. 在顶部菜单栏左上角处，选择服务所在地域：
   - **中国内地**：选择该地域将跳转到**DDoS高防（新BGP）**控制台。
   - **非中国内地**：选择该地域将跳转到**DDoS高防（国际）**控制台。

     您可以通过切换地域分别管理和配置DDoS高防（新BGP）和DDoS高防（国际）实例。在使用DDoS高防服务时，请确认您已选择正确的地域。
3. 在左侧导航栏，选择**接入管理 > 端口接入**。
4. 在**端口接入**页面，选择要操作的DDoS高防实例。
5. 定位到要操作的转发规则，单击其**DDoS防护策略**列下的**配置**。


6. 单击**源限速**下的**设置**。


7. 在**源限速设置**对话框，完成限速配置。

   以下图中配置为例，配置生效后，访问该高防端口的源并发连接不能超过50000个/秒，超过的源IP将被限速。如果勾选**源并发连接60秒内5次超限，将该源IP加入黑名单**，则DDoS高防将统计每个超限源IP在1分钟内的超限次数。如果大于5次，该源IP将被加入黑名单，所有来自该源IP的请求将被丢弃。

   源新建连接限速、源PPS限速和源带宽限速的使用方法同上。更多信息，请参见设置DDoS防护策略。

8. 单击**确定**，使配置生效。

# 7.4. 设置静态页面缓存

DDoS高防在流量清洗中心集成了网页缓存技术，在为网站业务提供DDoS防护的同时还可以加速网站静态页面的访问。

## 前提条件

您的网站业务已接入增强功能套餐的DDoS高防实例。更多信息，请参见添加网站。

## 背景信息

网站业务接入DDoS高防后，您可以为网站开启静态页面缓存功能。开启静态页面缓存后，DDoS高防将从客户端对网站域名的访问请求中自动检测符合缓存策略的资源类型，并缓存相关页面。已缓存页面将被写入网站对应的DDoS防护节点中，在下次客户端请求页面时直接返回，提升页面访问速度。

静态页面缓存也支持自定义规则，方便您只为指定的页面开启缓存功能。

## 操作步骤

1. 登录DDoS高防控制台。
2. 在顶部菜单栏左上角处，选择服务所在地域：
   - **中国内地**：选择该地域将跳转到**DDoS高防（新BGP）**控制台。
   - **非中国内地**：选择该地域将跳转到**DDoS高防（国际）**控制台。

     您可以通过切换地域分别管理和配置DDoS高防（新BGP）和DDoS高防（国际）实例。在使用DDoS高防服务时，请确认您已选择正确的地域。
3. 在左侧导航栏，选择**DDoS防护实验室 > 网站加速**。
4. 在页面上方，选择要操作的域名。

   > 注意　域名必须关联了增强功能的DDoS高防实例，才可以开启静态页面缓存。

5. 定位到**静态页面缓存**区域，选择一种缓存**模式**，并开启**状态**开关。

   不同缓存模式的说明如下：
   - **标准**：被请求页面包含静态文件资源（CSS、JS、TXT）时，缓存相关页面。
   - **增强**：缓存所有被请求的页面。
   - **不缓存**：不缓存任何被请求的页面。

   为域名开启静态页面缓存后，缓存策略对域名下所有URI生效。

   如果您希望只对指定的URI开启缓存功能，建议您将缓存**模式**设置为**不缓存**，并参照下一步自定义静态页面缓存规则。
6. （可选）为域名下指定URI（目录）自定义静态页面缓存规则。
   i. 在**静态页面缓存**区域，单击**设置**。

ii. 单击**新增规则**。

> **说明** 最多允许添加3条自定义规则。


iii. 在**新增规则**对话框，完成以下规则配置，并单击**确定**。


| 参数 | 说明 |
| --- | --- |
| **规则名称** | 设置规则的名称。<br>支持使用英文字母、数字或下划线（_）。长度不允许超过128个字符。 |
| **URI** | 要缓存的页面的URI。<br>**URI**中无需填写请求参数，且不支持使用通配符。<br>示例：填写 `/a/` 表示 `<域名>/a/` 路径下的所有页面。 |
| **模式** | 选择要应用的缓存策略。可选项：**标准模式**、**强力模式**、**不缓存**。<br>关于不同缓存策略的含义，请参见步骤5中的说明。 |
| **过期时间缓存** | 选择缓存的有效时间。默认为**遵循源站配置**（表示使用与源站配置的缓存时间相同的配置），也可以设置为**1小时**、**1天**、**10天**、**30天**。 |

成功添加针对指定URI的自定义规则后，自定义规则将优先于针对域名的缓存策略生效。您可以在规则列表中查看新增的规则，并根据需要**编辑**、**删除**规则。您也可以单击**刷新缓存**，手动强制刷新对应页面的缓存。

# 7.5. 定制场景策略

DDoS高防的定制场景策略允许您在特定的业务突增时段（例如新业务上线、双11大促销等）选择应用独立于通用防护策略的定制防护策略模板，保证适应业务需求的防护效果。您可以根据需要设置定制场景策略。

## 背景信息

定制场景策略提供基于业务场景定制的DDoS防护策略模板供您选择。创建定制场景策略时，您只需根据业务场景类型选择要应用的模板，并配置要应用策略的活动对象（支持域名和高防IP）。定制场景策略在有效时间段内生效。策略生效期间，域名或高防IP的DDoS防护策略以防护策略模板的定义为准，暂时忽略通用防护策略配置。

> **注意** 如果业务无明显突增且容易遭受攻击，建议您采用通用防护策略，不要启用定制场景防护策略。

**支持的策略模板**

目前仅提供**重大活动**策略模板，后续将开放其他基于场景定制的策略模板。

**应用示例**

当网站有重大活动时，网站整体请求量较大，流量表现会与平时差异较大。这种情况下，如果使用正常业务模式的DDoS防护策略，可能带来误杀。建议您使用**定制场景策略**的**重大活动**模板，该模板会在指定的活动期间自动调整DDoS防护策略。自动调整策略的逻辑如下：

- 活动开始时，自动记录**AI智能防护**、**频率控制**的开关配置，并自动将这两个功能的开关设置为关闭，避免误伤。
- 活动结束时，自动将这两个功能的开关恢复为先前配置。
- 如果您在活动期间手动开启这两个功能的开关，则以手动配置为准。

## 操作步骤

1. 登录DDoS高防控制台。
2. 在顶部菜单栏左上角处，选择服务所在地域：
   - **中国内地**：选择该地域将跳转到**DDoS高防（新BGP）**控制台。
   - **非中国内地**：选择该地域将跳转到**DDoS高防（国际）**控制台。

     您可以通过切换地域分别管理和配置DDoS高防（新BGP）和DDoS高防（国际）实例。在使用DDoS高防服务时，请确认您已选择正确的地域。
3. 在左侧导航栏，选择**防护设置 > 定制场景策略**。
4. 单击**创建场景策略**。
5. 在**创建场景策略**对话框，完成以下配置，并单击**确定**。


| 参数 | 说明 |
| --- | --- |
| **策略名称** | 为策略命名。 |
| **策略模板** | 选择要应用的定制策略模板，目前仅支持**重大活动**。 |

| 参数 | 说明 |
| --- | --- |
| **生效时间段** | 选择策略的生效时间段。<br>**说明** 如果同一个策略模板下存在多个策略，则这些策略的**生效时间段**不允许重合。 |

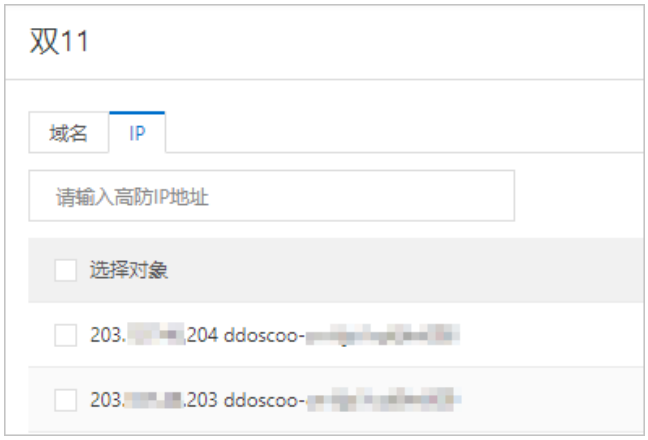
成功添加策略后，策略默认开启。您可以在策略列表中查看新建的策略，并通过策略的**状态**了解策略是否生效。不同策略状态的说明如下：

- **等待生效**：当前时间还未到活动生效时间段。
- **生效中**：活动策略下发生效中，需要1~2分钟完成。
- **运行生效**：当前时间处于活动生效时间段。
- **过期失效**：当前时间晚于活动生效时间段。
- **已被禁用**：策略被禁用。即使当前时间处于活动生效时间段内，活动策略也不会生效。

6. 在策略列表中，定位到新建的策略，单击其操作列下的**配置对象**。


7. 从已接入DDoS高防的域名或DDoS高防IP中选择要应用当前策略的域名或IP，并单击**确定**。

**说明** 如果您的业务是网站业务且通过域名接入DDoS高防，建议您为对应域名应用策略；如果您的业务是四层业务，且不是通过域名接入DDoS高防，建议您为对应IP应用策略。




成功应用策略后，策略的**防护对象**信息将会自动更新。您可以将光标放置在防护对象信息上，查看应用当前策略的域名或IP。


策略名称
策略模板
生效间段
状态
防护对象
8
重大活动
2020年1月16日 00:00:00 - 2020年1月17日 00:00:00
等待生效
0个
春节大促
重大活动
2020年1月24日 00:00:00 - 2020年1月25日 00:00:00
等待生效
0个
双11
重大活动
2020年1月29日 00:00:00 - 2020年1月30日 00:00:00
等待生效
2个

# 8.安全服务

## 8.1. 概述

安全服务帮助您处理DDoS高防使用过程中遇到的问题，协助您完成网站接入、防护配置、安全分析等任务。

根据服务形式和计费方式的不同，DDoS高防提供以下安全服务：

- 安全专家指导服务：加入阿里云企业安全服务钉钉群，免费享受安全专家通过钉钉为您提供的一对一指导服务。

  您必须使用钉钉沟通工具，才可以使用该服务。关于钉钉，请参见阿里巴巴钉钉官网首页。
- 高防产品托管服务：通过预付费方式开通高防产品托管服务，可以享受阿里云原厂安全服务团队提供的全面的DDoS高防技术支持，例如接入设置、防护策略优化、监控与告警设置、安全报表定制等。

  该服务适用于需要外包专业人员协助进行安全产品服务运营的用户，采用专属钉钉群、电话会议等方式进行交付。

  使用该服务时，您需要开通服务授权，允许阿里云安全服务专家查看您的业务场景数据，以便提供有针对性的防护咨询和日志数据深度分析建议。更多信息，请参见开通高防安全服务授权。

## 8.2. 安全专家指导服务

阿里云DDoS高防支持通过钉钉服务群为您提供免费的一对一专家指导服务。您在使用DDoS高防过程中遇到任何问题时，都可以通过DDoS高防管理控制台的专家指导服务入口获取7*24的DDoS高防产品帮助服务。

### 前提条件

- 已经购买DDoS高防实例。更多信息，请参见购买DDoS高防实例。
- 已经在手机移动端安装并注册使用钉钉聊天应用。更多信息，请参见阿里巴巴钉钉官网。

### 背景信息

安全专家指导服务支持以下两种方式：

- 加入阿里云官方钉钉服务群咨询问题：适合咨询相对简单的问题，加入临时的官方产品服务群，不需要多个业务相关人员参与提问。
- 创建并使用企业专属钉钉服务群咨询问题：适合企业级用户，可以创建7*24的专属服务群，随时咨询产品使用过程中的任何问题，支持邀请多个企业业务相关人员共同参与提问。

### 加入阿里云官方钉钉服务群咨询问题

1. 登录DDoS高防控制台。
2. 在左侧导航栏底部，单击 

图标。

   > 注意　只有当您已购买DDoS高防实例后，控制台才会显示**有问题，找专家**。

3. 打开手机钉钉应用，扫描显示的二维码，申请加入DDoS高防产品问题咨询群。
   成功加入DDoS高防产品问题咨询群后，您可以在群里直接咨询使用DDoS高防时遇到的问题。钉钉群内的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高防产品使用过程中遇到的任何问题。

## 创建并使用企业专属钉钉服务群咨询问题

> **注意** 该方式只向2020年06月后首次购买DDoS高防实例的用户开放。如果您在2020年06月之前已经购买过DDoS高防实例，则不支持通过DDoS高防控制台创建企业专属钉钉服务群，建议您通过阿里云官方钉钉服务群，联系我们帮助您创建专属钉钉服务群。更多信息，请参见加入阿里云官方钉钉服务群咨询问题。

1. 登录DDoS高防控制台。
2. 在左侧导航栏底部，单击 有问题，找专家 图标。

> **注意** 只有当您已购买DDoS高防实例后，控制台才会显示**有问题，找专家**。

3. 创建企业专属钉钉服务群 。
   i. 单击**使用钉钉注册手机号**。

   > **说明** 只有在2020年06月后首次购买DDoS高防实例，控制台才会显示**使用钉钉注册手机号**。

   ii. 填写企业专属钉钉服务群的注册信息。


| 参数 | 说明 |
| --- | --- |
| **钉钉注册手机号** | 填写成功注册了钉钉应用的中国手机号码。 |
| **钉钉昵称** | 填写使用当前手机号码注册的钉钉名称。 |
| **企业名称** | 填写您的公司简称。示例：阿里云。 |

iii. 单击**提交**。
提交申请后，钉钉会立即为您创建专属的阿里云企业安全服务群，群名称默认为“【安全】*企业名称*企业服务群”。

> **说明** 如果您收到申请建群失败的提示，建议您通过扫描二维码的方式联系我们，安全专家收到您的问题后将会第一时间与您沟通。更多信息，请参见加入阿里云官方钉钉服务群咨询问题。

成功创建并加入阿里云企业安全服务群后，您可以在群里直接咨询使用DDoS高防时遇到的问题。钉钉群内的安全专家将通过钉钉为您提供一对一指导服务，帮助您快速解决DDoS高防产品使用过程中遇到的任何问题。

4. （可选）邀请企业中其他业务相关业务人员加入企业专属安全服务群。
   i. 单击**使用钉钉注册手机号**。
   ii. 填写要加入企业专属安全服务群的钉钉用户的信息。


| 参数 | 说明 |
| --- | --- |
| **钉钉注册手机号** | 填写成功注册了钉钉应用的中国手机号码。 |
| **钉钉昵称** | 填写使用当前手机号码注册的钉钉名称。 |

iii. 单击**提交**。

提交申请后，您申请的钉钉用户将自动加入到企业专属安全服务群，并可以在群内直接提问。

# 8.3. 高防产品托管服务

云盾DDoS高防支持产品托管服务。开通高防产品托管后，您可以在阿里云安全产品专家的帮助下完成高防接入配置、安全监控和巡检、防护策略优化，并享有安全事件响应、安全咨询、安全培训和案例分享、安全报告等服务。

## 概述

高防产品托管由阿里云原厂安全服务团队提供技术支持，面向云盾DDoS防护用户提供产品托管服务。高防产品托管帮助您更有效地使用高防产品保护Web资产，降低业务安全风险，减少运维人力投入。

高防产品托管适用于已开通阿里云DDoS高防产品，但缺乏业务持续监控能力和缺少可应对安全漏洞风险的安全工程师的业务场景。该服务适合需要外包专业人员协助来进行安全产品服务运营的用户。

> **说明** 由于托管服务的部分工作内容（包括但不局限于防护策略优化、监控和预警设置、安全报告定制等）需要使用DDoS高防日志服务，如果您未购买DDoS高防日志服务，上述托管服务可能存在无法交付的风险。建议您在选购高防产品托管服务的同时，购买DDoS高防日志服务功能。更多信息，请参见概述。

## 服务内容

高防产品托管为您提供完整的高防产品接入和使用支持，下表描述了具体的服务内容。

| 服务类型 | 描述 |
| --- | --- |
| 接入配置 | • 在高防上配置保护对象的域名策略。<br>• 协助用户配置和上传HTTPS证书（用户可自行上传）。<br>• 按照客户要求配置合理的防护阈值。<br>• 协助用户配置ECS和SLB的源站保护策略。<br>• 产品适配和访问测试验证。<br>• 用户保护域名变化时，调整相关配置。 |
| 防护策略优化 | • 在高防上的业务出现异常时，提供诊断和排错服务。<br>• 基于攻防日志，优化用户安全防护策略和配置。<br>• 安全事件响应时，调整防护策略和提供方案，帮助用户缓解事件影响。<br>• 提供故障处理、CC防护规则、精准访问控制规则、数据风控等高防防护配置建议。 |
| 监控和预警 | • 系统自动化监控高防集群可用性故障。<br>• 系统自动化监控DDoS攻击导致的高危时事件。<br>• 人工在线判断和过滤监控事件预警。 |
| 安全报告 | • 根据用户要求提供定制化安全报告内容。<br>• 提供服务日报和服务月报，其中日报包括当天操作信息，月报包括操作数据和攻防数据分析。 |

## 安全事件响应时间

开通高防产品托管后，当您遇到安全事件需要紧急协助时，服务团队响应您的时间遵循下表描述。

安全事件响应时间

| 序号 | 优先级 | 定义 | 响应时间 |
| --- | --- | --- | --- |
| 1 | 危险 | 用户核心业务严重受损或完全不可用 | 15分钟 |
| 2 | 紧急 | 用户核心业务出现非全局异常 | 30分钟 |
| 3 | 高 | 用户非核心业务严重受损或不可用 | 2小时 |
| 4 | 中 | 用户非核心业务出现非全局异常 | 4小时 |

| 序号 | 优先级 | 定义 | 响应时间 |
| --- | --- | --- | --- |
| 5 | 低 | 用户日常技术咨询 | 8小时 |

### 服务交付方式

下表描述了高防产品托管的服务交付方式。

服务交付方式

| 类别 | 描述 |
| --- | --- |
| 服务交付方式 | 远程在线服务 |
| 服务语言 | 中文和英语 |
| 服务周期 | 与用户购买周期一致 |
| 支持的服务渠道 | • 电子邮件<br>• 钉钉<br>• 电话 |

### 定价和售卖方式

高防产品托管服务支持通过预付费方式开通，并且可按月或者按年续费。 购买高防产品托管服务，立即前往高防产品托管服务售卖页。

> **注意** 由于服务支持系统和服务人力资源投入的特殊性，高防产品托管服务在支付购买后暂不支持退款。

# 8.4. 产品托管服务授权

## 8.4.1. 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。

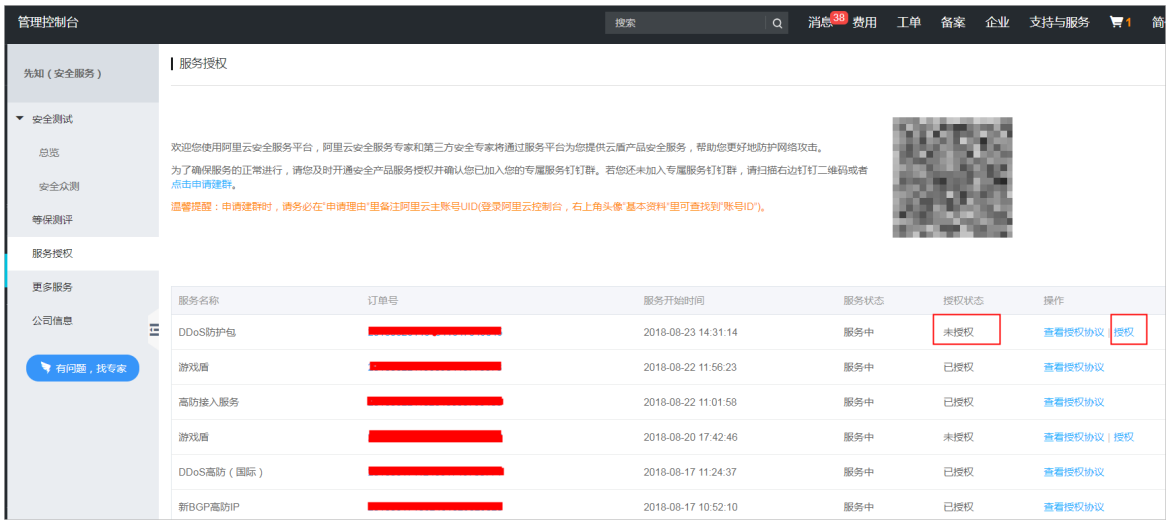
> **说明** 您必须已购买或开通云盾高防产品，才能享受高防安全专家服务。

### 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。


## 执行结果

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。

# 8.4.2. 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

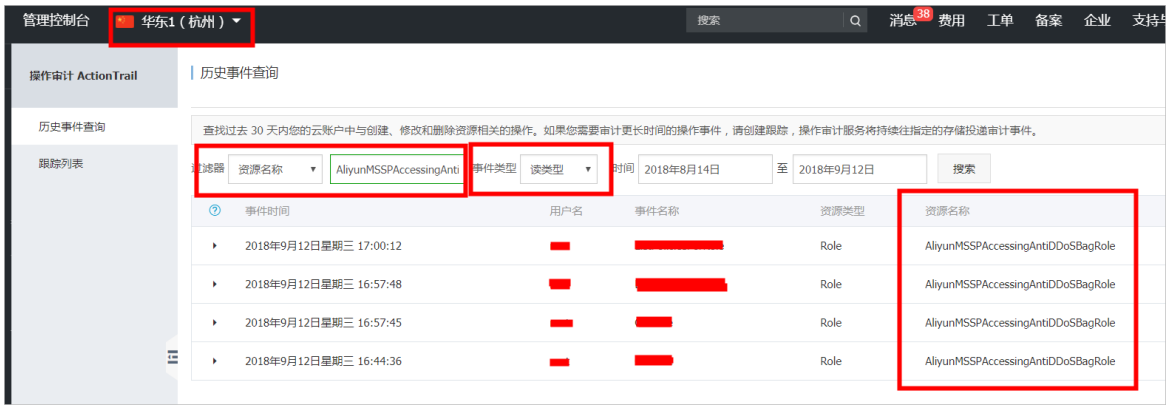
1. 登录操作审计管理控制台，选择**华东1（杭州）**。


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。

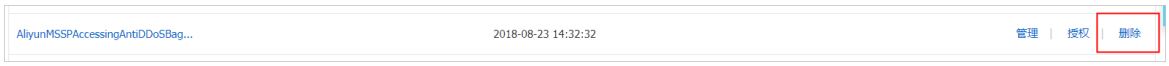

4. 单击**查看事件**可查看该事件的详细参数。

# 8.4.3. 取消高防安全服务授权

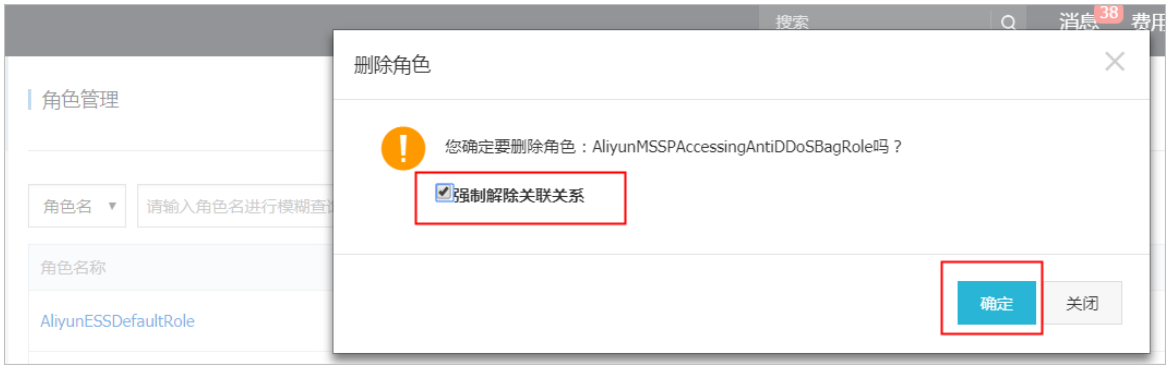
高防安全服务授权开通后，您可以随时在访问控制（RAM）管理控制台中删除高防安全服务的授权角色，取消高防安全服务授权。

## 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。


## 执行结果

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**。

# 9.最佳实践

# 9.1. DDoS高防接入配置最佳实践

业务接入DDoS高防产品后，可以将攻击流量引流到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DDoS高防更好地保护您的业务。

## 接入配置流程概述

| 接入场景 | 接入配置流程 |
| --- | --- |
| **正常情况下的业务接入** | 1. 业务梳理<br>2. 准备工作<br>3. 接入和配置DDoS高防 |
| **业务遭受攻击时的紧急接入** | 参照正常情况下的业务接入配置流程操作前，必须先阅读了解紧急接入场景须知。 |

如果您对接入配置有疑问，建议您使用安全专家服务。更多信息，请参见安全专家服务。

## 步骤1：业务梳理

首先，建议您对需要接入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 | 操作建议 |
| --- | --- | --- |
| **网站和业务信息** | | |
| 网站或应用业务每天的流量峰值情况，包括Mbps、QPS | 判断风险时间点。 | 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域） | 判断非法攻击来源。 | 方便业务接入后配置DDoS高防的区域封禁策略。更多信息，请参见设置区域封禁（针对域名）。 |
| 业务是否为C/S架构 | 如果是C/S架构，进一步明确是否有App客户端、Windows客户端、Linux客户端、代码回调或其他环境的客户端。 | 无。 |
| 源站是否部署在非中国内地地域 | 判断所配置的实例是否符合最佳网络架构。 | 源站部署在非中国内地地域时，建议选购DDoS高防（国际）服务。更多信息，请参见什么是DDoS高防（新BGP&国际）。 |
| 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。 | 如果有，需要在源站上设置放行DDoS高防的回源IP。更多信息，请参见放行DDoS高防回源IP。 |

| 梳理项 | 说明 | 操作建议 |
| --- | --- | --- |
| 业务是否需要支持IPv6协议 | 无。 | 如果您的业务需要支持IPv6协议，建议您使用DDoS原生防护。更多信息，请参见什么是DDoS原生防护。 |
| 业务使用的协议类型 | 无。 | 用于后续业务接入DDoS高防时配置网站信息，需要选择对应的协议。 |
| 业务端口 | 无。 | 判断源站业务端口是否在DDoS高防的支持端口范围内。更多信息，请参见自定义服务器端口。 |
| 请求头部（HTTP Header）是否带有自定义字段且服务端拥有相应的校验机制 | 判断DDoS高防是否会影响自定义字段导致服务端业务校验失败。 | 如果有，请提交工单联系技术支持人员协助分析。 |
| 业务是否有获取并校验真实源IP机制 | 接入DDoS高防后，真实源IP会发生变化。请确认是否要在源站上调整获取真实源IP配置，避免影响业务。 | 如果需要，请参见配置DDoS高防后获取真实的请求来源IP。 |
| 业务是否使用TLS 1.0或弱加密套件 | 判断业务使用的加密套件是否支持。 | 完成业务接入后，根据需要设置TLS安全策略。具体操作，请参见自定义TLS安全策略。 |
| （针对HTTPS业务）服务端是否使用双向认证 | 无。 | DDoS高防暂不支持双向认证，需要变更认证方式。 |
| （针对HTTPS业务）客户端是否支持SNI标准 | 无。 | 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 | DDoS高防的HTTP和HTTPS默认连接超时时长为120秒。 | 如果您的业务有上传、登录等长会话需求，建议您使用基于七层的Cookie会话保持功能。 |
| 业务是否存在空连接 | 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。 | 如果有，请提交工单联系技术支持人员协助分析。 |
| 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。 | 无。 |
| 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。 | 无。 |
| **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。 | 无。 |
| 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。 | 无。 |

| 梳理项 | 说明 | 操作建议 |
| --- | --- | --- |
| 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。 | 无。 |
| 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。 | 更多信息，请参见设置频率控制。 |
| 用户群体属性 | 例如，个人用户、网吧用户、通过代理访问的用户。 | 用于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。 | 无。 |
| 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。 | 更多信息，请参见购买DDoS高防实例。 |
| 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。 | 无。 |
| 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。 | 无。 |
| 业务是否提供Web API服务 | 无。 | 如果提供Web API服务，不建议使用频率控制的攻击紧急防护模式。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。 | 无。 |

## 步骤2：准备工作

**注意** 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，您需要完成下表描述的准备工作。

| 业务类型 | 准备工作 |
| --- | --- |

| 业务类型 | 准备工作 |
| --- | --- |
| 网站业务 | • 准备需要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。<br>• 所接入的网站域名必须已完成ICP备案。更多信息，请参见ICP备案流程概述。<br>• 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。<br>• 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。<br>• 推荐在将网站业务接入前，完成压力测试。<br>• 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 | • 准备对外提供服务的端口、协议类型。<br>• 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。<br>• 推荐在将业务接入前，完成压力测试。 |

## 步骤3：接入和配置DDoS高防

1. 业务接入配置。

   > **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。具体操作，请参见更换源站ECS公网IP。

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

   - 网站类业务接入DDoS高防（新BGP&国际）
   - 非网站类业务接入DDoS高防（新BGP&国际）
   - 通过NS方式将网站类业务接入DDoS高防（新BGP）

2. 配置源站保护。

   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。具体操作，请参见设置源站保护。

3. 配置防护策略。
   - 网站域名类业务

- 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情况并相应配置频率控制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DDoS高防管理控制台的**安全总览**报表（具体操作，请参见查看安全总览），获取域名请求TOP URL、IP地址、访问来源IP、User-agent等参数信息，根据实际情况制定频率控制自定义规则（具体操作，请参见自定义频率控制防护规则），并观察防护效果。

    如果实际防护效果不佳，您可以联系阿里云安全服务专家（更多信息，请参见安全专家服务），协助您进一步分析日志并制定防护策略。

    > **注意** 由于**频率控制**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**频率控制**的默认防护模式。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**模式。
    >
    > 如果使用**频率控制**的**正常**模式仍发现误拦截现象，建议您使用白名单功能放行特定IP。

- （网站业务）AI智能防护

  由于AI智能防护策略中的**严格**模式存在对业务造成误拦截的可能性，且网站域名类业务接入对常见四层攻击已有天然的防护能力，请您不要使用网站业务AI智能防护中的**严格**模式，建议使用默认的**正常**模式。更多信息，请参见设置AI智能防护。

- 开启全量日志

  强烈建议您开启全量日志分析服务（具体操作，请参见快速上手）。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。

- **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四层AI智能防护的模式（具体操作，请参见设置四层AI智能防护），可有效提升针对网络四层CC攻击的防护效果。

  > **说明** 如果您的业务是API类型或存在集中单个IP访问（例如，办公网出口、单个服务器IP、高频率调用API接口业务等）的情况，请不要开启非网站业务AI智能防护策略的**严格**模式。如果确实需要使用**严格**防护模式，请联系阿里云技术支持人员确认情况后再启用，避免因误拦截造成业务无法访问。

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（具体操作，请参见设置端口DDoS防护策略）。在不完全清楚业务情况时，建议将源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，需要关闭空连接防护策略（具体操作，请参见设置端口DDoS防护策略），避免正常业务受到影响。


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*文件的方式进行本地测试。

   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（必检）** | |
| 1 | 接入配置域名是否填写正确。 |
| 2 | 域名是否备案。 |
| 3 | 接入配置协议是否与实际协议一致。 |
| 4 | 接入配置端口是否与实际提供的服务端口一致。 |
| 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DDoS高防实例的IP或其他服务的IP。 |

| 编号 | 检查项 |
| --- | --- |
| 6 | 证书信息是否正确上传。 |
| 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）。 |
| 8 | 证书链是否完整。 |
| 9 | 是否已了解DDoS高防（新BGP）实例的弹性防护计费方式。 |
| 10 | 协议类型是否启用Websocket、Websockets协议。 |
| 11 | 是否开启频率控制的攻击紧急和严格模式。 |
| **非网站端口类业务检查项（必检）** | |
| 1 | 业务端口是否可以正常访问。 |
| 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。 |
| 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DDoS高防实例的IP或其他服务的IP。 |
| 4 | 是否已了解DDoS高防实例（新BGP）实例的弹性防护计费方式。 |
| 5 | 是否开启四层AI智能防护的严格模式。 |

业务可用性验证项

| 编号 | 检查项 |
| --- | --- |
| 1（必检项） | 测试业务是否能够正常访问。 |
| 2（必检项） | 测试业务登录会话保持功能是否正常。 |
| 3（必检项） | （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。 |
| 4（必检项） | （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。 |
| 5（建议项） | 是否配置后端服务器获取真实访问源IP。 |
| 6（建议项） | （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。 |
| 7（必检项） | 测试TCP业务的端口是否可以正常访问。 |

5. 正式切换业务流量。

   必要检查项均检测通过后，建议采用灰度的方式逐个修改DNS解析记录，将网站业务流量切换至DDoS高防，避免批量操作导致业务异常。如果切换流量过程中出现异常，请快速恢复DNS解析记录。

   > **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. 配置监控告警。

建议您使用云监控对已接入DDoS高防进行防护的域名、端口和业务源站端口进行监控（具体操作，请参见设置DDoS高防报警规则），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DDoS高防（新BGP）的用户可以免费获得三个300 Gbps规格的抗D包（更多信息，请参见DDoS高防抗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 Gbps。绑定成功后，当日内（自然日）所遭受的抗D包防护规格内（300 Gbps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（新BGP）的弹性防护能力，请务必先查看DDoS高防（新BGP）的计费方式（更多信息，请参见弹性防护（按天后付费）），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。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，您可以查看DDoS高防管理控制台的**安全总览**报表（具体操作，请参见查看安全总览），根据攻击流量信息判断遭受的攻击类型：
     - DDoS攻击类型：在**实例**防护报表中有攻击流量的波动，且已触发流量清洗，但在**域名**防护报表中不存在相关联的波动。
     - CC攻击类型： 在**实例**防护报表中有攻击流量的波动，已触发流量清洗，且在**域名**防护报表中有相关联的波动。

     更多信息，请参见如何判断DDoS高防实例受到的攻击类型。
   - **业务访问延时或丢包**：

     针对源站服务器在中国内地以外地域、主要访问用户来自中国内地地域的情况，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DDoS高防管理控制台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。

## 紧急接入场景须知

如果您的业务已经遭受攻击，建议您在将业务接入DDoS高防时注意以下内容：

- 业务已遭受DDoS攻击

  一般情况下，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，建议您开启DDoS防护策略中的源、目的连接限速策略（具体操作，请参见设置端口DDoS防护策略）。

- 源站IP已被黑洞

  如果在接入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）。具体操作，请参见更换源站ECS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接入备案（更多信息，请参见接入备案流程），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、爬虫攻击时，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。具体操作，请参见安全专家服务。

### 安全专家服务

购买DDoS高防后，您可以在DDoS高防管理控制台通过钉钉扫描二维码直接联系阿里云安全服务专家。具体操作，请参见安全专家指导服务。

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。

# 9.2. 同时接入DDoS高防和Web应用防火墙

DDoS高防支持与阿里云Web应用防火墙一起使用，实现为网站业务同时防御DDoS攻击和Web应用攻击。本文介绍了网站业务同时接入DDoS高防和Web应用防火墙的配置方法。

### 前提条件

- 已开通DDoS高防（新BGP）或者DDoS高防（国际）实例。更多信息，请参见购买DDoS高防实例。
- 已开通Web应用防火墙实例。更多信息，请参见开通Web应用防火墙。

### 背景信息

网站业务同时接入DDoS高防和Web应用防火墙时，需要采用以下网络架构：DDoS高防（入口层，防御

DDoS攻击）->Web应用防火墙（中间层，防御Web应用攻击）->源站服务器（ECS、SLB、VPC、IDC等）。

> **说明** 应用上述架构后，访问请求将经过多层中间代理才到达源站，源站不能直接获取请求的真实来源IP。如果您需要获取访问请求的真实来源IP，请参见配置DDoS高防后获取真实的请求来源IP。

## 操作步骤

1. 网站业务接入Web应用防火墙（具体操作请参见添加域名）。

   在**填写网站信息**时，您需要选择**IP**类型的**服务器地址**，填写源站服务器对应的SLB公网IP、ECS公网IP或本地服务器IP，并将**WAF前是否有七层代理（高防/CDN等）**设置为**是**。


   成功添加域名后，您可以在Web应用防火墙控制台的**网站接入**页面获取域名对应的WAF **CName**地址。


2. 网站业务接入DDoS高防（具体操作请参见添加网站配置）。

   在**填写网站信息**时，您需要选择**源站域名**类型的**服务器地址**，并填写上一步获取的WAF **CName**地址。


成功添加网站后，您可以在DDoS高防控制台的**域名接入**页面获取域名对应的DDoS高防**CNAME**地址。


3. 在域名的DNS解析服务商处修改域名的DNS解析，将域名解析指向上一步获取的DDoS高防**CNAME**地址（具体操作请参见修改DNS解析接入网站业务）。
   完成上述配置后，网站业务流量会先经过DDoS高防清洗，然后转发到Web应用防火墙过滤Web攻击，最后只有正常的业务流量被转发到源站服务器。

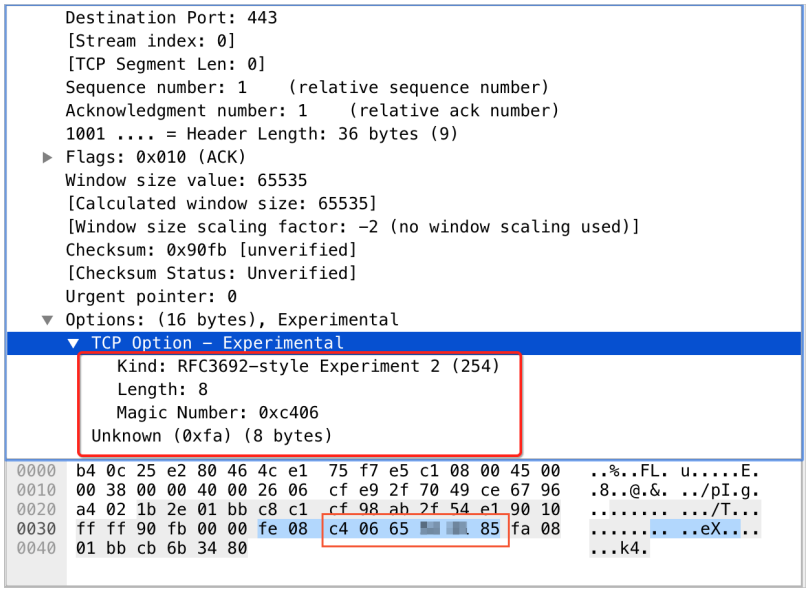
# 9.3. 配置DDoS高防后获取真实的请求来源IP

Web业务部署DDoS高防后，到达源站的所有业务流量都由DDoS高防转发，请求来源IP默认是DDoS高防实例的IP地址。本文介绍了这种情况下如何获取真实的请求来源IP。

## 配置端口接入的业务（非网站防护）

> **注意**
>
> - 2018年10月后创建的ECS实例，默认支持获取真实的请求来源IP，即在源站ECS服务器上看到的请求来源IP就是真实的访问源IP。
> - 2018年10月前创建的ECS实例，默认情况下无法获取真实的请求来源IP，您需要提交工单申请开通相关配置。

业务四层端口接入后，高防节点和源站经过三次握手，在最后一个ACK数据包的TCP Option中插入了源端口号和源IP等信息，共占6个字节。具体位置如下图所示。




其中，`Magic Number`表示端口号（使用十六进制表示，示例中为`c4 06`），通过端口号可以定位到IP地址信息（端口号后的连续四个字节，示例中为`65 ** ** 85`）。通过十六进制转为十进制，可以获得对应的端口号和IP地址（示例中端口为50182，源IP地址为101.***.***.133）。

根据业务的网络架构不同，获取真实请求来源IP的方式也不同，具体请参见下表说明。

| 网络架构 | 说明 |
| --- | --- |
| DDoS高防->阿里云ECS | • 通过TCP端口转发流量的情况，默认支持获取真实的请求来源IP，无需您做任何改动。源站服务器上看到的请求来源IP就是真实的访问源IP。<br>您可以基于请求来源IP和高防回源IP设置ECS的安全组策略，例如放行或拒绝指定IP的入方向流量。<br>• 如果您使用UDP端口转发，则ECS源站不支持获取真实的请求来源IP。 |
| DDoS高防->负载均衡SLB->阿里云ECS | • 通过TCP端口转发流量的情况，默认支持获取真实的请求来源IP，无需您做任何改动。源站服务器上看到的请求来源IP就是真实的访问源IP。<br>**说明** 您必须将DDoS高防的回源IP添加到负载均衡SLB的访问控制白名单中。更多信息，请参见放行DDoS高防回源IP、开启访问控制。<br>• 如果您使用UDP端口转发，则ECS源站不支持获取真实的请求来源IP。<br>**说明** 如果您修改了ECS的私网IP地址或者进行过ECS过户，则不支持获取真实的请求来源IP。遇到这种情况，请您提交工单联系我们协助解决。 |
| DDoS高防->非阿里云ECS服务器 | 部分情况下支持获取真实的请求来源IP。更多信息，请参见云外主机获取真实请求来源IP。 |

## 配置域名接入的业务（网站防护）

当七层代理服务器（例如DDoS高防）将用户的访问请求转发到后端服务器时，源站看到的请求来源默认是七层代理服务器（例如DDoS高防）的回源IP，而真实的请求来源IP被记录在HTTP头部的 `X-Forwarded-For` 字段中，格式为 `X-Forwarded-For：用户真实IP，高防代理IP` 。

如果访问请求到后端服务器间经过了一台以上代理服务器（例如经过WAF、CDN等代理服务器），则HTTP头部的 `X-Forwarded-For` 字段记录了真实的请求来源IP和所有经过的代理服务器IP，格式为 `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，常见的Web应用服务器都可以通过 `X-Forwarded-For` 字段的内容获取真实的请求来源IP。

针对不同的编程语言，常用的获取 `X-Forwarded-For` 内容的方式如下：

- ASP

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

- ASP.NET（C#）

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

- PHP

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

- JSP

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

获取到 `X-Forwarded-For` 字段的内容后，以英文逗号（,）作为分隔符，截取其中的第一个IP地址，即可获取真实的请求来源IP。

> **说明** 关于常见Web服务器（例如Nginx、IIS 6、IIS 7、Apache、Tomcat）获取真实访问IP的具体配置方法，请参见获取客户端真实IP。

# 9.4. 云外主机获取真实请求来源IP

非阿里云ECS服务器（主要指线下IDC服务器）配置了DDoS高防后，由于业务请求流量先经过DDoS高防清洗过滤再转发到源站服务器，源站无法直接获取真实的请求来源IP。这种情况下建议您使用本文介绍的方法，在源站上配置toa模块来获取真实的请求来源IP。

## 适用场景

下表列举了支持获取真实的请求来源IP的场景。

| 适用场景 | 描述 | 是否支持获取请求来源IP |
| --- | --- | --- |
| 高防-七层SLB-云下IDC服务器 | 源站部署在IDC服务器上。业务流量先经过DDoS高防清洗后，由七层SLB转发到达源站（IDC服务器）。 | 支持 |
| 高防-四层SLB-云下IDC服务器 | 源站部署在IDC服务器上。业务流量先经过DDoS高防清洗后，由四层SLB转发到达源站（IDC服务器）。 | 不支持 |

| 适用场景 | 描述 | 是否支持获取请求来源IP |
| --- | --- | --- |
| 高防-云下IDC服务器 | 源站部署在IDC服务器上。业务流量经过DDoS高防清洗后到达源站（IDC服务器）。 | 支持 |

## 适用的操作系统

本文介绍的方法适用于以下操作系统：

- Redhat Linux
- CentOS 6.x
- CentOS 7.x

## 操作步骤

执行操作前，请阅读以下注意事项：

> **注意**
> - 建议您先在测试环境中执行本文描述的操作，观察环境稳定后再在正式环境中进行配置。
> - 建议您保留原有的内核，如果出现重启失败，可以切换到原有内核执行系统恢复。

1. 根据您的服务器系统类型，下载相应的内核安装文件。
   - CentOS 7.x系统：kernel-3.10.0-957.21.3.el7.toa.x86_64.rpm
   - CentOS 6.x或Redhat Linux系统：
     - kernel-firmware-2.6.32-696.13.2.el6.centos.plus.toa.x86_64
     - kernel-2.6.32-696.13.2.el6.centos.plus.toa.x86_64
2. 安装内核。
   - CentOS 7.x系统

     定位到安装文件目录，执行以下命令：

     ```
     sudo yum localinstall kernel-3.10.0-957.21.3.el7.toa.x86_64.rpm
     ```

     > **说明** 建议您使用 `yum localinstall` 命令安装内核，避免出现依赖问题。您也可以执行 `sudo rpm -ivh kernel-3.10.0-957.21.3.el7.toa.x86_64.rpm` 命令进行安装。

   - CentOS 6.x或Redhat Linux系统

     定位到安装文件目录，执行以下命令：

     ```
     sudo rpm -ivh kernel-firmware-2.6.32-696.13.2.el6.centos.plus.toa.x86_64.rpm
     sudo rpm -ivh kernel-2.6.32-696.13.2.el6.centos.plus.toa.x86_64.rpm
     ```

> **说明**
>
> - 如果系统中的kernel-firmware版本大于或等于2.6.32-696.13.2.el6.centos.plus.toa，只需要执行上述第二行命令。
> - 如果安装过程中出现依赖错误，可以尝试在 `rpm` 命令中加上额外参数 `--nodeps` 。
> - 如果内核版本大于toa内核版本，可以尝试在 `rpm` 命令中加上额外参数 `--force` ，进行强制安装。

3. 设置toa模块，开启系统启动时自动加载功能。
   i. 创建文件*/etc/sysconfig/modules/toa.modules*，并在文件中添加以下内容：
   - CentOS 7.x系统：

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

   - CentOS 6.x或Redhat Linux系统：

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

   ii. 执行以下命令，授予*toa.modules*文件可执行权限：

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

4. 执行 `reboot` 命令，重启系统。
   安装完成后，主机能够正常获取真实访问源IP。

   如果仍无法获取真实访问源IP，建议您执行 `lsmod|grep toa` 命令检测toa模块的加载情况。如果toa模块未加载，您可以执行 `modprobe toa` 命令手动加载。加载成功后，您可以查看服务端访问日志，重新测试主机能否获取真实的访问源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？

  建议您保留原有的内核，如果出现重启失败，可以切换到原有内核执行系统恢复。

# 9.5. 切换业务关联的DDoS高防实例

如果您在现有DDoS高防实例到期后，重新购买了新的DDoS高防实例，需要在业务不中断的前提下将已配置的业务迁移到新的DDoS高防实例进行防护，则您可以修改已接入域名的配置，为域名关联新的DDoS高防实例。

## 操作步骤

1. 登录DDoS高防控制台。
2. 在顶部菜单栏左上角处，选择服务所在地域：
   - **中国内地**：选择该地域将跳转到**DDoS高防（新BGP）**控制台。
   - **非中国内地**：选择该地域将跳转到**DDoS高防（国际）**控制台。

     您可以通过切换地域分别管理和配置DDoS高防（新BGP）和DDoS高防（国际）实例。在使用DDoS高防服务时，请确认您已选择正确的地域。
3. 在左侧导航栏，选择**接入管理 > 域名接入**。
4. 定位到要切换DDoS高防实例的域名，单击其操作列下的**编辑**。
5. 重新选择当前网站要关联的DDoS高防**实例**，并单击**确定**。

   > 说明
   > - 不支持同时关联**标准功能**和**增强功能**套餐下的实例。
   > - 一个域名最多可以关联一种**功能套餐**下的8个实例。


6. 在弹出的对话框中确认已选择的DDoS高防实例，并单击**确定**。


## 执行结果

切换DDoS高防实例后，原有DDoS高防实例上的配置将下发到新的DDoS高防实例，原有业务将由新关联的DDoS高防实例进行防护。

# 9.6. 接入DDoS高防后如何设置源站保护

业务接入DDoS高防后，到达源站服务器的业务流量都由DDoS高防转发，这种情况下您可以设置源站的访问控制策略，例如只允许DDoS高防回源IP的入方向流量，达到保护源站的目的。不同接入场景下DDoS高防源站保护的设置方法不同，您可以根据本文介绍选择适合您当前网络架构的方法。

**说明** 设置源站保护主要针对小流量CC攻击和Web攻击有防护效果，对于防护大规模的DDoS攻击意义并不大。设置源站保护并不能防止没有经过DDoS高防的流量对源站直接发动的DDoS攻击（甚至将源站打入黑洞）。

| Web业务的网络架构 | 源站保护设置说明 |
| --- | --- |
| DDoS高防->阿里云ECS | 该架构下，转发到源站的流量的来源IP为DDoS高防的回源IP。<br>建议您在源站ECS的安全组中设置源站保护策略，只放行DDoS高防的回源IP段，并拒绝其他所有来自非DDoS高防回源IP段的访问请求。您可以在DDoS高防控制台获取高防的回源IP段。详细内容，请参见放行DDoS高防回源IP 。 |
| DDoS高防->非阿里云ECS源站服务器 | 该架构下，转发到源站的流量的来源IP为DDoS高防的回源IP。<br>建议您在源站服务器上的安全软件（例如iptables、防火墙等）中设置源站保护策略，只放行DDoS高防的回源IP段，并拒绝其他所有来自非DDoS高防回源IP段的访问请求，实现源站保护。 |
| DDoS高防->负载均衡SLB（4层）->阿里云ECS | 该架构下，转发到源站的流量的来源IP为DDoS高防的回源IP。<br>建议您在负载均衡SLB实例上设置源站保护策略，将DDoS高防的回源IP段添加到SLB的访问控制白名单中，并开启访问控制，实现只允许DDoS高防的回源IP访问SLB实例。更多信息，请参见开启访问控制。 |
| DDoS高防->负载均衡ALB（7层）->阿里云ECS | 该架构下，转发到源站ECS的流量的来源IP为负载均衡ALB的回源IP。<br>建议您在负载均衡实例上设置源站保护策略，将DDoS高防的回源IP段添加到ALB的访问控制白名单中，并开启访问控制，实现只允许DDoS高防的回源IP访问ALB实例。更多信息，请参见访问控制。 |
| DDoS高防->Web应用防火墙、阿里云CDN->阿里云ECS | 该架构下，转发到源站ECS的流量的来源IP为WAF或者CDN的回源IP。<br>建议您在WAF、CDN中设置相应的源站保护策略。更多信息，请参见设置源站保护。 |
| DDoS高防->Web应用防火墙、阿里云CDN->非阿里云ECS源站服务器 | |

# 9.7. 端口接入模式下源站ECS的最佳配置方案

当使用非网站接入（端口接入TCP业务）、并且源站为阿里云ECS或VPC时，可能存在访问流量绕过DDoS高防直接到达源站的风险。 为规避该风险，为您提供以下配置建议：

- 在源站ECS的安全组中，配置“只放行高防回源网段”的规则，并拒绝其他非DDoS高防回源IP访问ECS源站。

  您可以在DDoS高防控制台获取高防的回源IP段。相关内容，请参见放行DDoS高防回源IP。
- 如果您有其他信任IP地址需要直接访问ECS源站时（如办公室内网出口IP等），可以在ECS安全组中配置对应的放行规则。

# 9.8. 源站IP暴露的解决办法

业务配置DDoS高防后，如果存在攻击绕过DDoS高防直接攻击源站的情况，说明源站IP地址可能已经暴露，需要您更换源站服务器的IP地址。

## 排查源站IP暴露的原因

更换源站服务器的IP地址前，请务必确认您已经消除了所有可能暴露源站IP的因素，避免源站IP更换后再次暴露。您可以从以下方面进行排查：

- 源站服务器上是否存在木马、后门等安全隐患。

  推荐您使用阿里云云安全中心服务检查和修复服务器的安全漏洞。更多信息，请参见什么是云安全中心。

- 源站服务器上是否存在没有配置DDoS高防的其他服务，例如邮件服务器的MX记录、BBS记录等除Web记录以外的记录。

  > **注意** 请仔细检查网站域名的DNS解析记录，确认没有任何记录直接解析到源站服务器的IP地址。

- 是否存在网站源码信息泄露。例如 `phpinfo()` 指令中可能包含的IP地址等泄露。
- 是否存在恶意扫描。您可以在配置DDoS高防后设置源站保护，在源站服务器上只放行DDoS高防回源IP的入方向流量。具体操作请参见接入DDoS高防后如何设置源站保护。

## 更换源站IP

确认已消除所有可能暴露源站IP的因素后，您可以更换源站服务器的IP地址。具体操作请参见更换 ECS IP。

如果您不想更换源站IP或已经更换过源站IP但是仍存在IP暴露的情况，建议您在后端ECS服务器前部署一台负载均衡SLB服务器（具体操作请参见负载均衡快速入门）。您可以使用以下网络架构：客户端->DDoS高防->SLB->ECS。

采用这种架构后，即使攻击者直接攻击源站，导致源站IP被黑洞，通过DDoS高防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，DDoS高防实例的IP仍然可以通过负载均衡服务器访问源站。

> **说明** 应用上述网络架构时，您需要在DDoS高防控制台中填写负载均衡服务器的IP作为服务器地址。