阿里云
DDoS高防IP

新BGP高防IP

文档版本：20191022

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. **阿里云文档中所有内容，包括但不限于图片、架构设计、页面布局、文字描述，均由阿里云和/或其关联公司依法拥有其知识产权，包括但不限于商标权、专利权、著作权、商业秘密等。非经阿里云和/或其关联公司书面同意，任何人不得擅自使用、修改、复制、公开传播、改变、散布、发行或公开发表阿里云网站、产品程序或内容。此外，未经阿里云事先书面同意，任何人不得为了任何营销、广告、促销或其他目的使用、公布或复制阿里云的名称（包括但不限于单独为或以组合形式包含“阿里云”、“Aliyun”、“万网”等阿里云和/或其关联公司品牌，上述品牌的附属标志及图案或任何类似公司名称、商号、商标、产品或服务名称、域名、图案标示、标志、标识或通过特定描述使第三方能够识别阿里云和/或其关联公司）。**
6. **如若发现本文档存在任何错误，请与阿里云取得直接联系。**

通用约定

格式	说明	样例
	该类警示信息将导致系统重大变更甚至故障，或者导致人身伤害等结果。	 **禁止:** 重置操作将丢失用户配置数据。
	该类警示信息可能会导致系统重大变更甚至故障，或者导致人身伤害等结果。	 **警告:** 重启操作将导致业务中断，恢复业务时间约十分钟。
	用于警示信息、补充说明等，是用户必须了解的内容。	 **注意:** 权重设置为0，该服务器不会再接受新请求。
	用于补充说明、最佳实践、窍门等，不是用户必须了解的内容。	 **说明:** 您也可以通过按Ctrl + A选中全部文件。
>	多级菜单递进。	单击设置 > 网络 > 设置网络类型。
粗体	表示按键、菜单、页面名称等UI元素。	在结果确认页面，单击**确定**。
`Courier字体`	命令。	执行`cd /d C:/window`命令，进入Windows系统文件夹。
*## *	表示参数、变量。	`bae log list --instanceid` *`Instance_ID`*
[]或者[a|b]	表示可选项，至多选择一个。	`ipconfig [-all|-t]`
{}或者{a|b}	表示必选项，至多选择一个。	`switch {active|stand}`

目录

1 产品简介

1.1 什么是新BGP高防IP

新BGP高防IP服务采用中国大陆地域独有的T级八线BGP带宽资源，可防御超大流量DDoS攻击。相比静态IDC高防IP服务，新BGP高防IP天然具有灾备能力、线路更稳定、访问速度更快。

新BGP高防IP服务具有以下优势：

- **拥有中国大陆地域最大的BGP带宽资源，最高防护带宽达到1.5T，可以应对超大流量攻击。**
- **拥有中国大陆地域最优质的BGP带宽资源，BGP线路覆盖电信、联通、移动、教育等运营商线路，平均访问时延仅20ms左右。**
- **只需要一个IP，即可满足中国大陆地域内不同运营商线路的快速访问和DDoS防护需求。**

与静态IDC高防IP服务对比

	静态IDC高防IP服务（电信、联通、移动线路）	静态IDC高防IP服务（BGP线路）	新BGP高防IP服务
运营商覆盖	仅覆盖电信、联通和移动线路。	除了覆盖电信、联通和移动线路外，还能覆盖众多中小运营商。	除了覆盖电信、联通和移动线路外，还能覆盖众多中小运营商。
线路质量	中国大陆地域平均访问时延在30ms左右，且对于小运营商可能存在跨网访问。	中国大陆地域平均访问时延在20ms左右，且不存在运营商跨网访问。	中国大陆地域平均访问时延在20ms左右，且不存在运营商跨网访问。
专线回源	不支持。通过互联网回源，存在回源时延。	对于阿里云上的业务，提供专线回源，回源延时可忽略；对于非阿里云内业务，仍通过互联网回源。	对于阿里云上的业务，提供专线回源，回源延时可忽略；对于非阿里云内业务，仍通过互联网回源。
灾备能力	机房故障时，四层流量无法进行自动调度；七层流量自动调度受限于DNS解析生效时间，无法立即生效。	通过BGP路由实现全部流量自动调度，故障响应切换时间可达秒级左右。	通过BGP路由实现全部流量自动调度，故障响应切换时间可达秒级左右。
IP数量	包含2个以上IP，配置工作量相对繁琐。	仅1个IP，配置工作量较少。	仅1个IP，配置工作量较少。

	静态IDC高防IP服务（电信、联通、移动线路）	静态IDC高防IP服务（BGP线路）	新BGP高防IP服务
最高防护能力	提供最高1T的防护能力（仅支持电信和联通线路）。	提供最高100G的防护能力。	提供最高1.5T的防护能力。
四层防护能力	支持防御SYN Flood、ACK Flood、ICMP Flood、畸形包等流量攻击；防御空链接、真实肉鸡连接等攻击。	与静态IDC高防IP服务的防护能力一致。	与静态IDC高防IP服务的防护能力一致。
七层防护能力	支持防御CC攻击。	支持防御CC攻击。	支持防御CC攻击。

新BGP高防IP的适用场景

如果您有以下DDoS防护需求，建议选购新BGP高防IP服务：

- **对线路质量有较高要求，包括访问时延、灾备能力、覆盖运营商线路范围等要求。**
- **需要20G以上保底防护带宽的BGP线路高防IP服务。**
- **具有大流量攻击防护需求（300G以上）。**

相关文档

- **购买新*BGP*高防*IP***
- **计费方式**

2 产品定价

2.1 计费方式

新BGP高防IP服务提供T级BGP线路的DDoS防护能力，帮助您解决超大流量DDoS攻击（特别是300G以上的大流量攻击）。如果您的业务对访问时延比较敏感，建议您使用新BGP高防IP服务。本文介绍了新BGP高防IP服务的计费方式。

基础防护（按月-预付费）

DDoS防护能力	线路	费用
30Gbps	八线BGP	· 标准功能：20,800 元/月 · 增强功能：28,800 元/月
60Gbps	八线BGP	· 标准功能：46,800 元/月 · 增强功能：54,800 元/月
100Gbps	八线BGP	· 标准功能：328,000 元/年（包年优惠价） · 增强功能：424,000 元/年（包年优惠价）
300Gbps	八线BGP	· 标准功能：528,000 元/年（包年优惠价） · 增强功能：624,000 元/年（包年优惠价）
400Gbps	八线BGP	· 标准功能：968,000 元/年（包年优惠价） · 增强功能：1,064,000 元/年（包年优惠价）
500Gbps	八线BGP	· 标准功能：3,753,600 元/年（包年优惠价） · 增强功能：3,849,600 元/年（包年优惠价）
600Gbps	八线BGP	· 标准功能：4,467,600 元/年（包年优惠价） · 增强功能：4,563,600 元/年（包年优惠价）

> **说明:**
>
> - 关于不同功能套餐间的区别，请参见功能套餐说明。
> - 如果您需要更高的DDoS防护能力，请通过工单联系我们。

同时，新BGP高防实例默认包含以下业务规格。

> **说明:**
> 如果实际业务需要超出实例的默认业务规格，您可以通过升级实例或在购买实例时对相应规格进行扩展。

业务规格	规格说明	默认情况	扩展单价（元/月）
防护端口数	实例支持添加的TCP/UDP端口数量。	50个	每5个端口： 250 元/月
防护域名数	实例支持添加的HTTP/HTTPS域名数量。	50个 **说明:** 所有域名所属的一级域名总数不超过5个。	• 标准功能套餐：每10个域名300 元/月 • 增强功能套餐：每10个域名500 元/月 **说明:** 每增加10个域名可增加一个一级域名。
业务带宽	实例支持处理的无攻击情况下最大业务流量。	100 Mbps	每Mbps：100 元/月 **说明:** 当实例的总业务带宽规格超出600 Mbps时，超出部分的扩展业务带宽可享受优惠价（每Mbps：75 元/月）。
业务QPS	实例支持处理的无攻击情况下最大HTTP/HTTPS业务的并发请求速率。	3,000 QPS	每100 QPS： 1,000 元/月

弹性防护（按天-后付费）

新BGP高防实例的弹性防护费用，按照前一日实际发生的超出保底防护带宽的攻击流量部分的峰值（即选取当日内所遭受的DDoS攻击中的最大值后，扣除该实例的保底防护带宽值，得到超出部分的流量峰值）所对应的计费区间进行计算，生成后付费账单。

说明:

如果您将新BGP高防实例的弹性防护带宽设置为与保底防护带宽一致，则不会产生任何后付费账单，但您的新BGP高防实例也将不具备弹性防护能力。

例如，您的新BGP高防实例的保底防护带宽规格是30Gb，其弹性防护带宽设置为100Gb。当日该实例遭受两次DDoS攻击，其中一次攻击的峰值为80Gb，另一次攻击的峰值为40Gb，两次攻击均超过保底防护带宽。系统将选取当日所遭受的最大攻击峰值80Gb，并扣除实例的保底防护带宽30Gb，得到50Gb，按照“40 Gb<攻击峰值≤50 Gb”的计费区间计算当日所产生的弹性防护费用，即6,400元。

注意事项

- 当日实际发生的DDoS攻击峰值不大于所购买的保底DDoS防护能力，则不会产生任何后付费。
- 当日实际发生的DDoS攻击峰值超过所设置的弹性防护带宽，则不会产生后付费账单。即如果当日实际遭受的DDoS攻击导致所防护的IP被黑洞，则不收取弹性防护费用。
- 当日的弹性防护费用账单一般在第二天上午八点至九点生成。

计费区间	弹性防护费用
0 Gb<攻击峰值≤5 Gb	¥ 800／天
5 Gb<攻击峰值≤10 Gb	¥ 1,200／天
10 Gb<攻击峰值≤20 Gb	¥ 2,200／天
20 Gb<攻击峰值≤30 Gb	¥ 3,600／天
30 Gb<攻击峰值≤40 Gb	¥ 4,880／天
40 Gb<攻击峰值≤50 Gb	¥ 6,400／天
50 Gb<攻击峰值≤60 Gb	¥ 7,800／天
60 Gb<攻击峰值≤70 Gb	¥ 9,200／天
70 Gb<攻击峰值≤80Gb	¥ 10,600／天
80Gb<攻击峰值≤100Gb	¥ 11,800／天
100Gb<攻击峰值≤150Gb	¥ 14,600／天
150Gb<攻击峰值≤200Gb	¥ 21,600／天
200Gb<攻击峰值≤300Gb	¥ 28,000／天

计费区间	弹性防护费用
300Gb<攻击峰值≤400Gb	¥ 40,000／天
400Gb<攻击峰值≤500Gb	¥ 50,000／天
500Gb<攻击峰值≤600Gb	¥ 60,000／天
600Gb<攻击峰值≤700Gb	¥ 70,000／天
700Gb<攻击峰值≤800Gb	¥ 80,000／天
800Gb<攻击峰值≤900Gb	¥ 90,000／天
900Gb<攻击峰值≤1000Gb	¥ 100,000／天
1000Gb<攻击峰值≤1100Gb	¥ 110,000／天
1100Gb<攻击峰值≤1200Gb	¥ 120,000／天
1200Gb<攻击峰值≤1300Gb	¥ 130,000／天
1300Gb<攻击峰值≤1400Gb	¥ 140,000／天
1400Gb<攻击峰值≤1500Gb	¥ 150,000／天

不支持退款声明

阿里云新BGP高防包年包月服务不支持提前退订，也不适用五天无理由退款。若您已使用了新BGP高防实例，一概不支持退款。

更多信息

选择业务带宽规格

您可以根据所有已经或将要接入新BGP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。

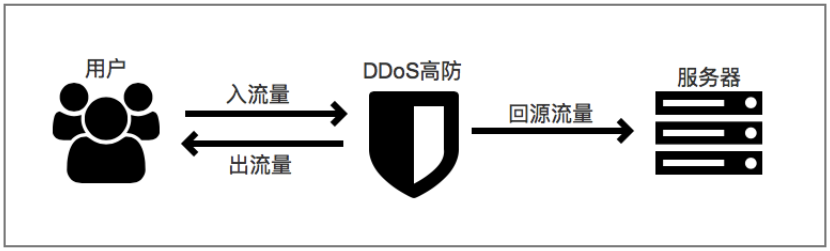
说明:
一般情况下，网络出方向的流量会比较大。

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它流量监控工具来评估您的实际业务流量大小。

说明:
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新BGP高防进行防护。在业务正常访问（未遭受攻击）时，新BGP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，新BGP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。



假设您需要将三个网站业务接入新BGP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。

选择防护域名规格

每10个域名数规格包含1个一级域名。即新BGP高防实例默认支持添加50条域名配置记录，且仅支持接入5个不同的一级域名。

例如，默认情况下，您可以添加五个一级域名（例如，`abc.com`），且为这些域名本身和它们的子域名或泛域名（例如，`www.abc.com`，`*.abc.com`，`mail.abc.com`，`user.pay.abc.com`，`x.y.z.abc.com`等）添加50条域名配置记录。

 说明:

所添加的这些域名（包括一级域名`abc.com`）都将占用实例的防护域名数。

如果您想要添加更多的一级域名或它们的子域名接入新BGP高防实例进行防护，您需要扩展防护域名数。假设您已经添加五个不同的一级域名或其子域名进行防护，当您尝试添加另一个一级域名或其子域名进行防护时，您将收到以下域名数量限制提示：

当前主域名个数有限制，请升级服务，扩展防护域名数。

这种情况下，您需要升级新BGP高防实例额外增加10个防护域名数量。

2.2 功能套餐说明

新BGP高防IP提供标准功能和增强功能两种套餐供您选择。增强功能套餐在标准功能套餐的基础上，额外提供网站加速缓存、非标准业务端口、区域流量封禁等增强功能，增强新BGP高防IP的

业务接入能力和DDoS攻击防护能力。您可以根据业务的情况和安全防护需求，选择适合的功能套餐。

购买新BGP高防IP实例时，系统默认选择标准功能套餐，您可以选择增强功能套餐来获得更强大的业务接入能力和DDoS攻击防护能力。增强功能套餐的售价为8,000元/月，即选择增强功能套餐将在标准功能套餐同规格实例的基础上增加8,000元/月的增强功能费用。

对于已购买的标准功能套餐实例，您可以通过升级新BGP高防IP实例规格为该实例开通增强功能。

说明:
新购或升级增强功能套餐后，对于已配置接入的网站域名业务您需要编辑域名配置关联增强功能套餐的新BGP高防IP实例，为网站域名业务使用增强功能。

标准功能与增强功能套餐

增强功能套餐在标准功能套餐的基础上提供更强大的业务接入能力和攻击防护能力。

功能分类	功能项	功能描述	标准功能套餐	增强功能套餐
防护算法	流量型攻击防护	支持常见的流量型DDoS攻击防护，包括畸形报文攻击防护和各类流量型Flood攻击防护。	✓	✓
	资源耗尽型攻击防护	支持常见的网络四层/七层资源耗尽型CC攻击防护，例如HTTP GET Flood、HTTP POST Flood攻击等。 详细信息，请参见防护HTTP(S) Flood攻击。	✓	✓
	AI智能防护	· 支持网络七层AI智能CC防护，缓解应用层精巧型CC攻击。 · 支持网络四层AI智能CC防护，缓解TCP连接耗尽型攻击。 详细信息，请参见#unique_11。	✓	✓

功能分类	功能项	功能描述	标准功能套餐	增强功能套餐
防护规则	黑白名单	针对每个接入防护的域名业务支持最多200条访问IP白名单和200条访问IP黑名单规则配置。 详细信息，请参见设置网站访问黑白名单。	✓	✓
	精准访问控制	支持HTTP协议精准匹配防护规则。 详细信息，请参见设置精准访问控制规则。	针对每个接入防护的域名业务支持配置最多五条规则，且仅支持IP、URL、Referer、User-Agent字段	针对每个接入防护的域名业务支持配置最多十条规则
	区域IP封禁	针对每个接入防护的域名业务的访问流量支持按区域进行封禁。 详细信息，请参见封禁特定区域IP访问。	✗	✓
业务接入	HTTP（80/8080）、HTTPS（443/8443）标准端口转发	支持HTTP（80/8080）、HTTPS（443/8443）业务的DDoS攻击防护。	✓	✓
	HTTP、HTTPS非标准端口转发	支持HTTP、HTTPS非标准端口（不限于80、8080、443、8443端口）业务的DDoS攻击防护。 说明: 每个实例支持最多配置10不同非标端口的转发。	✗	✓

功能分类	功能项	功能描述	标准功能套餐	增强功能套餐
其它	静态页面缓存	支持网站静态页面加速缓存。 说明： 目前，自定义缓存规则处于公测阶段，每个接入防护的域名业务支持配置最多三条规则。 详细信息，请参见加速网站静态页面访问。	✗	✓

2.3 购买新BGP高防IP

本文介绍了开通新BGP高防IP实例的具体操作。

操作步骤

1. 访问阿里云新*BGP*高防*IP*购买页面，并登录您的阿里云账号。
2. 根据您的业务需要，在基本配置区域选择保底防护带宽、弹性防护带宽、业务带宽。
   - 保底防护带宽：指新BGP高防IP实例的保底防护带宽。根据所选择的保底防护带宽及购买时长，生成预付费账单。
   - 弹性防护带宽：指新BGP高防IP实例的最高弹性防护带宽。对于超出保底防护带宽的攻击进行弹性防护，并根据当时实际发生的超出保底防护带宽攻击峰值生成后付费账单。

     说明：

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

- **业务带宽：指非DDoS攻击状态下新BGP高防IP实例所支持的正常业务消耗带宽。**

3. 在高级配置区域，选择所需的功能套餐，设置防护域名数、业务QPS、端口数。

- **功能套餐：指新BGP高防IP实例提供标准功能套餐和增强功能套餐供您选择。**

说明:

关于各功能套餐的具体介绍，请参见功能套餐说明。

- **防护域名数：指新BGP高防IP实例支持接入防护的HTTP/HTTPS域名数量。**

说明:

每10个域名包含1个一级域名（且仅限1个一级域名）和该一级域名的子域名或泛域名。

- 业务QPS：指新BGP高防IP实例支持处理的无攻击情况下最大HTTP/HTTPS业务的并发请求速率。
- 端口数：指新BGP高防IP实例支持的最大转发端口数量，即通过TCP/UDP协议转发支持的最大条目数。

4. 选择购买数量和购买时长，单击立即购买，完成支付。

预期结果

关于新BGP高防IP的详细计费说明，请查看*新BGP高防IP计费方式*。

2.4 升级新BGP高防IP实例规格

您购买新BGP高防IP实例后，如果所购买的实例规格（如功能套餐、保底防护带宽、防护域名数、端口数或业务带宽等）已无法满足您的实际业务需要，您可以随时在云盾新BGP高防IP控制台升级当前高防实例规格。

背景信息

升级实例规格支持升级至增强功能套餐，扩展保底防护带宽、防护域名数、端口数和业务带宽。升级当前新BGP高防IP实例规格，您需要补齐升级差价。支付完成后，新BGP高防IP实例规格升级即时生效。

说明:

不支持降低已购买新BGP高防IP实例的规格（包括功能套餐、保底防护带宽、防护域名数、端口数和业务带宽）。

升级功能套餐，增加防护域名数、端口数、业务带宽所产生的差价部分按以下方式计算：

- **功能套餐：升级增强功能套餐按 8,000 元/月的单价与当前服务剩余时长计算差价。**
- **防护域名数：新增防护域名按每 10 个域名 300 元/月（增强功能套餐实例按每 10 个域名 500 元/月）的价格与当前服务剩余时长计算差价。**
- **端口数：新增端口按 50 元/月的单价与当前服务剩余时长计算差价。**
- **业务带宽： 扩展业务带宽按 100 元/月的单价（每增加 1 M）与当前服务剩余时长计算差价。**

  说明:

  新BGP高防IP实例的业务带宽采用分阶段定价。业务带宽在100 M - 600 M（含600 M）区间内，每 1 M 按 100 元 / 月的单价计算；业务带宽超出600 M以上的部分每 1 M按 75 元 / 月的单价计算。
- **业务QPS：扩展业务带宽按每 100 QPS 1,000 元/月的价格与当前服务剩余时长计算差价。**

操作步骤

1. **登录云盾新*BGP*高防*IP*控制台。**
2. **定位到管理 > 实例列表，选择待升级的新BGP高防IP实例，单击升级。**

3. 在配置变更页面，选择功能套餐，扩展保底防护带宽、防护域名数、端口数、业务带宽。

4. 完成支付，升级后的新BGP高防IP实例规格配置即时生效。

3 快速入门

3.1 防护网站业务

3.1.1 概述

本文将指导您在开通新BGP高防IP后，快速部署和使用新BGP高防，为您的网站配置DDoS防护和CC攻击防护。

使用新BGP高防防护网站业务时，您可以按照以下步骤进行操作。

任务名	描述
步骤1：添加网站配置	在新BGP高防IP控制台，为要防护的网站创建网站配置，为其关联新BGP高防IP实例和设置流量转发信息。
步骤2：业务接入新BGP高防配置	通过修改接入新BGP高防的域名的解析记录，将网站访问流量牵引至新BGP高防IP实例。 完成切换后，接入防护的域名的访问请求都会先经过新BGP高防清洗，再转发到您的源站服务器，从而实现由新BGP高防IP实例帮助您防御DDoS攻击流量。
步骤3：设置DDoS防护策略	业务接入新BGP高防IP后，默认启用DDoS智能防御模式，无需您进行额外操作。在遇到异常情况或特殊需求时，您可以选择调整DDoS防护策略。 支持调整的DDoS防护策略包括：清洗模式、黑白名单、黑洞解封、流量封禁。
步骤4：设置CC防护策略	业务接入新BGP高防IP后，您可以为被防护的网站启用CC安全防护，并配置CC防护策略，防御针对网站页面的CC攻击。 支持配置的CC防护策略包括：黑白名单、CC安全防护。
步骤5：使用安全报表与日志	业务接入新BGP高防IP后，您可以在新BGP高防IP控制台，使用安全报表和日志功能查看防护数据。

3.1.2 步骤1：添加网站配置

要使用已开通的新BGP高防IP实例防护您的网站，您必须首先在新BGP高防IP中添加网站配置。添加网站配置无需您额外启用实例或选择高防节点，只要配置网站信息，将网站业务接入新BGP高防IP实例进行防护即可。

前提条件

已开通新BGP高防IP实例。已开通的实例可以在新BGP高防IP控制台，管理 > 实例列表中查看。关于如何开通服务，请参见购买新BGP高防IP。

操作步骤

1. 登录云盾新BGP高防IP控制台。
2. 在左侧导航栏，单击管理 > 网站配置。
3. 在网站配置页面，单击添加网站。

4. 在添加网站页面，完成填写网站信息配置。配置说明见下表。

配置项	描述
规格	选择功能套餐规格。取值： · 标准功能 · 增强功能

配置项	描述
实例	根据您在规格中选择的功能套餐类型显示对应的新BGP高防IP实例供您选择。 **说明:** 如果无可选实例，表示您当前无可用的该功能套餐规格的新BGP高防IP实例。您可以选择新购增强功能套餐实例或升级已有的标准功能套餐实例。 为将要接入的网站域名业务关联对应的新BGP高防IP实例。 **说明:** 一个域名最多支持关联8个新BGP高防IP实例，且不支持关联不同功能套餐的实例。
网站	填写要防护的网站域名。 **说明:** · 根据域名命名规则，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）以及连接符（-）组成，但是域名的首位必须是字母或数字。 · 支持填写泛域名，如`*.aliyun.com`。新BGP高防将自动匹配该泛域名对应的子域名。 · 如果同时存在泛域名和精确域名配置（如`*.aliyun.com`和`www.aliyun.com`），新BGP高防优先使用精确域名所配置的转发规则和防护策略。
协议类型	选择网站支持的协议类型，可选值： · HTTP（默认勾选） · HTTPS（默认勾选） · Websocket · Websockets **说明:** 如果要防护的网站支持HTTPS加密认证，则必须勾选HTTPS。同时，您可以根据网站实际所支持的协议类型勾选其它协议类型。

配置项	描述
启用HTTP2	如果您的业务支持HTTP2.0协议，可开启该开关进行防护。 **说明:** 启用HTTP2防护，需要符合以下要求： · 您的网站域名配置已关联增强功能套餐的新BGP高防实例。 · 您已勾选HTTPS协议类型。
服务器地址	选择源站地址类型，并指定源站服务器地址。支持的源站地址类型包括以下两种： · 源站IP：如果选择源站IP类型，支持配置最多20个源站IP地址。配置多个源站IP后，新BGP高防IP实例将以IP Hash的方式转发网站访问流量至源站，自动实现源站的负载均衡。 · 源站域名：如果您在部署新BGP高防IP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实例分配给源站的CNAME地址。 具体配置方法，请参见高防IP+云盾WAF同时使用最佳实践。

配置项	描述
服务器端口	根据您所选择的协议类型指定相应端口。 **说明:** 转发端口与服务器端口保持一致。 · 协议类型为HTTP或Websocket时，默认服务器端口为80。 · 协议类型为HTTPS或Websockets时，默认服务器端口为443。 **说明:** HTTP2.0协议的端口与HTTPS端口保持一致。 支持添加自定义端口。您可以单击自定义，并从可选端口范围中，选择配置默认端口以外的端口。 · 标准功能套餐实例：可选的HTTP/Websocket端口范围为80，8080；可选的HTTPS/Websockets端口范围为443，8443。 · 增强功能套餐实例：支持特定非标端口，具体支持范围请参见自定义非标端口。 

5. 单击添加。

预期结果

成功添加网站配置，自动跳转到修改DNS解析任务页；您可以单击返回网站列表，在网站配置列表中看到新添加的网站配置。

新BGP高防为每个网站配置生成一个关联高防IP，用于更新网站的DNS解析A记录，从而将网站访问请求转发到新BGP高防IP实例进行清洗。

后续步骤

- 步骤2：业务接入新BGP高防配置
- 上传HTTPS证书：若您的网站支持HTTPS协议，您必须上传HTTPS证书，才能使新BGP高防正常清洗HTTPS业务流量。

3.1.3 步骤2：业务接入新BGP高防配置

本文以阿里云云解析DNS为例，介绍如何在添加新BGP高防网站配置后，手动修改防护域名的DNS解析A记录，将您的网站业务切换至已配置的新BGP高防IP。

前提条件

修改DNS解析前，您需要完成以下任务：

- 添加网站配置。具体操作请参见步骤1：添加网站配置。
- 如果您的源站服务器已经部署了其他厂商的防火墙，请关闭防火墙或将新BGP高防IP的所有回源地址加入防火墙的白名单。 具体操作请参见放行新BGP高防回源IP。

  将网站访问流量切换至新BGP高防IP后，您网站的正常访问流量经过所配置的新BGP高防IP实例后，将通过这些回源IP地址转发至源站服务器。因此，如果新BGP高防IP的回源地址未被加入防火墙的白名单中，访问流量可能被防火墙错误拦截，导致网站无法访问。
- 验证转发配置。强烈建议您在切换网站访问流量前，验证并确认新BGP高防IP实例转发配置已经生效。具体操作请参见网站配置生效测试。

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。若您使用其他DNS服务商的域名解析服务，请登录服务商系统，将防护域名的解析A记录值更新为关联的高防IP。

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）的方式接入新BGP高防。具体操作请参见*NS*方式接入网站业务。

假设在步骤1添加网站配置中，您添加的防护域名为`bgp.ddostest.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A记录的具体步骤。

操作步骤

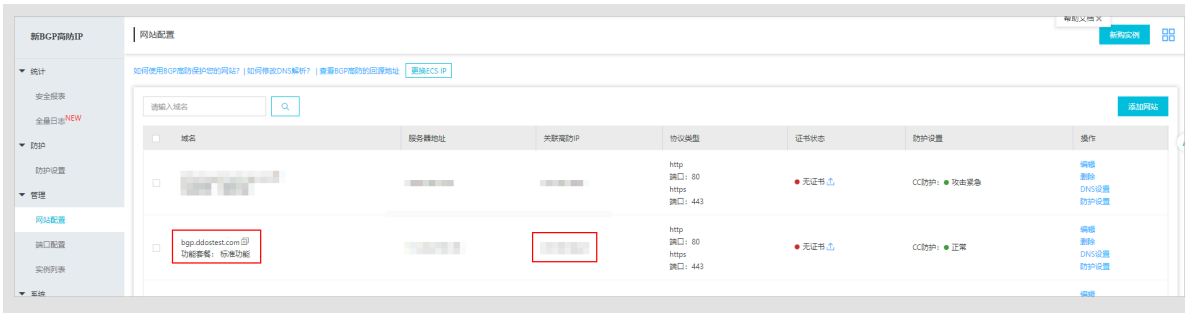
1. 登录阿里云云解析*DNS*控制台阿里云云解析*DNS*控制台。
2. 在域名解析页面，定位到要操作的域名（本示例中为`ddostest.com`），单击其操作列下的解析设置。

3. 在解析设置页面，定位到要修改的解析A记录（本示例中，即主机记录为bgp的A记录），单击其操作列下的修改。

> **说明:**
> 如果要操作的解析A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，将记录值修改为域名的关联高防IP。

> **说明:**
> 当您在新BGP高防IP控制台成功添加域名配置后，新BGP高防为域名分配一个关联高防IP。您可以在新*BGP*高防*IP*控制台新*BGP*高防*IP*控制台，管理 > 网站配置页面，查看已添加域名的关联高防IP。具体请参见步骤1：添加网站配置。



5. 单击确定，等待修改后的解析设置生效。

后续步骤

步骤3：设置DDoS防护策略

3.1.4 步骤3：设置DDoS防护策略

业务接入新BGP高防IP后，默认启用DDoS智能防御模式，无需您进行额外操作。在遇到异常情况或特殊需求时，您可以选择调整DDoS防护策略。

前提条件

添加网站配置。具体操作请参见步骤1：添加网站配置。

背景信息

支持调整的DDoS防护策略包括：

DDoS防护策略类型	描述
清洗模式	智能防御模式开启后，需要3天来学习业务流量并建立防御模型；有攻击的话，可以通过源新建连接自动限速功能来辅助防御，3天后智能防御达到最佳防护效果。如果正常模式下的防护效果没有达到预期，您可以尝试调整智能防御模式为严格模式。
黑白名单	对于已知的访问量较大的恶意IP，您可以将这类IP添加至黑名单，直接拦截其访问请求；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，您可以将这类IP添加至白名单，直接放行其访问请求。
黑洞解封	对于已加入新BGP高防防护的网站，如果因为其保底防护带宽或弹性带宽不足被突发大流量攻击造成黑洞，您可以在新BGP高防控制台使用黑洞解封来快速恢复业务。
流量封禁	当您遭遇特大流量攻击，且发现攻击流量有超过最大防护能力的趋势时，建议您考虑使用流量封禁，对新BGP高防IP实例中的电信/联通线路的海外流量实行主动封禁。

操作步骤

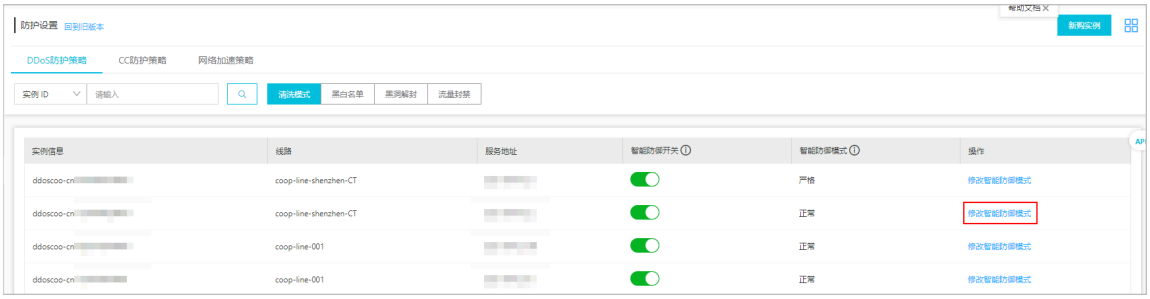
1. 登录**云盾新BGP高防IP控制台**。
2. 在左侧导航栏，单击管理 > 网站配置。
3. 在网站配置列表中，定位到要操作的域名，单击其操作列下的防护设置。

4. 在防护设置页面，打开DDoS防护策略页签，根据需要执行以下操作：

- 清洗模式

  定位到要操作的实例，单击操作列下的修改智能防御模式，并在修改智能防御模式对话框中选择一个清洗模式。支持的清洗模式包括：

  - 宽松：针对攻击特征显著的恶意IP进行防护，防护效果弱，误杀率低。
  - 正常：针对攻击特征明显、可疑的恶意IP进行防护，平衡防护效果及误杀率。
  - 严格：针对有攻击特征的请求IP进行防护，攻击防御效果强，但存在一定数量的误杀。



- 黑白名单

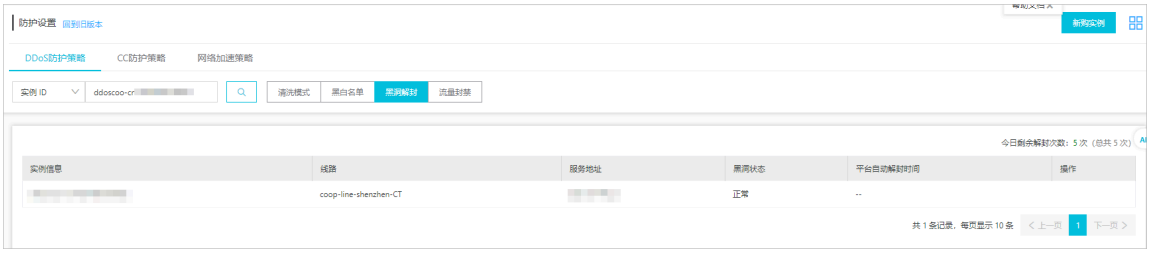
说明:

黑白名单的配置仅针对单个网站域名生效，而不是针对整个新BGP高防IP实例。

单击手动添加，添加黑名单或白名单。具体操作请参见设置网站访问黑白名单。

- **黑洞解封**

  对于处于黑洞状态下的实例，单击其操作列下的解封。具体操作请参见手动解除黑洞状态。



- **流量封禁**

  定位到要操作的实例，单击其操作列下的封禁，封禁电信或联通线路的海外流量。具体操作请参见主动封禁海外流量。

3.1.5 步骤4：设置CC防护策略

业务接入新BGP高防IP后，您可以为防护网站启用CC安全防护，防御针对网站页面的CC攻击。

前提条件

已添加网站配置。具体操作请参见步骤1：添加网站配置。

背景信息

新BGP高防IP提供的CC安全防护策略包括以下内容：

- **黑白名单：通过设置访问来源IP黑白名单，可以直接封禁来自黑名单IP访问请求，或者直接放行来自白名单IP的访问请求。**

- CC安全防护：通过开启CC安全防护，自动检测并阻断伪装成网站页面请求的CC攻击。您可以根据需要设置常规防护或者自定义防护。
  - 常规防护：根据业务需求，选用不同管控力度的防护模式进行防护。
  - 自定义防护：配置自定义防护规则，针对网站下具体页面的访问请求设置限速策略。

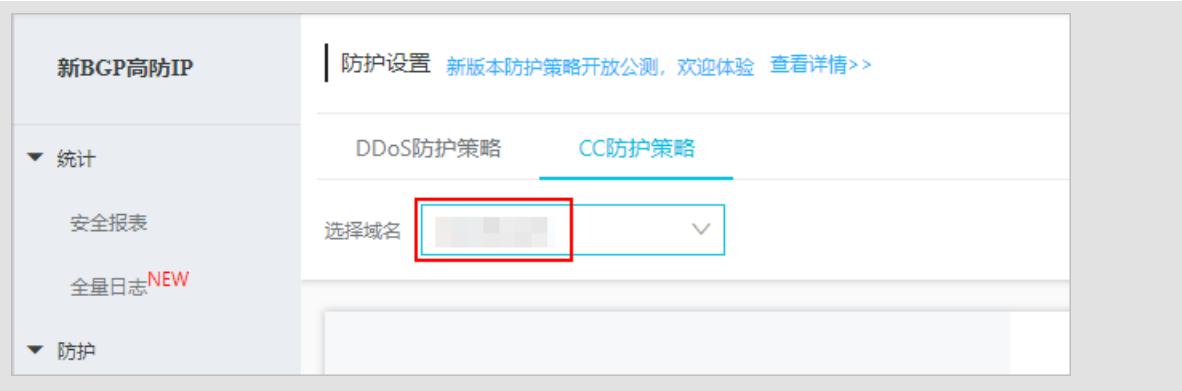
> **说明:**
> 目前，新版防护策略全面公测，欢迎您体验试用。新版防护策略公测期间，您的新BGP高防的CC防护策略默认仅包含黑白名单和CC安全防护功能。如果您想体验全新的区域封禁、精准访问控制、AI智能防护和网站加速缓存功能，推荐您切换至新版防护策略。具体操作请参见*#unique_32*。

操作步骤

1. 登录**云盾新*BGP*高防*IP*控制台**。
2. 在左侧导航栏，单击管理 > 网站配置。
3. 在网站配置列表中，定位到要操作的域名，单击其操作列下的防护设置。

4. 在防护设置页面，打开CC防护策略页签，根据需要执行以下操作：

> **说明:**
> CC防护策略针对防护域名生效；在配置CC防护策略前，请确认已选择正确的域名。



- **黑白名单**

  在黑白名单下，单击设置，并在黑白名单设置对话框中，分别添加黑名单IP和白名单IP。

说明:

支持使用IP或者IP/掩码格式，且支持添加最多200个黑名单IP和200个白名单IP。多个IP间以英文逗号（,）进行分隔。

- **CC安全防护**

  在CC安全防护下，打开状态开关，并根据业务需要选择合适的防护方式。

  - **常规防护**

    根据业务现状与需求，选择一种合适的防护模式：正常、攻击紧急、严格、超级严格。

    说明：

防护模式越严格，则对访问请求的管控力度越大，误杀量会有提高；建议您在正常模式无法缓解大量攻击的情况下，根据需要逐步切换更高强度的防护模式。更多信息，请参见防护*HTTP(S) Flood*攻击。

- 自定义规则

  a. 打开自定义规则开关，并单击设置。

  b. 在CC防护自定义规则页面，单击新增规则。

  c. 在新增规则对话框中，完成以下配置。

配置项	描述
规则名称	为规则命名。
URI	要防护的具体的页面地址。
匹配规则	判断访问请求是否计数的规则，可选值： ■ 完全匹配：访问请求的页面与防护URI完全相同时，进行计数。 ■ 前缀匹配：访问请求的页面的前缀与防护URI相同时，进行计数。
检测时长	判断访问来源IP是否命中的规则：当单一IP在检测时长内的访问计数超过单一IP访问次数时，则记作命中并触发阻断操作。
单一IP访问次数	

配置项	描述
阻断类型	访问来源IP命中规则后，触发的阻断操作类型，可选值： ■ 封禁：在指定时长内，封禁访问来源IP的访问请求。 ■ 人机识别：触发规则后，用重定向的方式去访问客户端，通过验证后才放行。

图例中规则配置说明：当单一IP在5秒内对防护域名下的`/login`页面的请求次数超过20次，则直接封禁该IP的访问请求；封禁时长为5分钟，5分钟后自动解除封禁。

d. 单击确定。

成功添加的规则出现在规则列表中，支持编辑和删除操作。

3.1.6 步骤5：使用安全报表与日志

业务接入新BGP高防后，您可以在新BGP高防IP控制台，使用安全报表和日志功能查看防护数据。

前提条件

- **已添加网站配置。具体操作请参见步骤1：添加网站配置。**
- **已将业务切换至新BGP高防。具体操作请参见步骤2：业务接入新BGP高防配置。**

操作步骤

1. **登录云盾新BGP高防IP控制台。**
2. **根据需要，选择执行以下操作：**

   - **查看安全报表**

     在左侧导航栏，单击统计 > 安全报表；在报表页面，根据页签选择要查看的报表类型：业务、DDoS攻击防护、CC攻击防护，查看对应报表记录。

每种报表都支持筛选功能，您可以指定要查看的时间范围，以及实例或IP、端口信息等。每种报表包含的信息见下表。

报表类型	支持查看的信息	支持的筛选项
业务	- in/out带宽趋势 - 并发连接数和新建连接数	- 时间 - 实例 - 高防IP - 转发端口
DDoS攻击防护	- 流量图（回源流量和清洗流量） - DDoS攻击记录	- 时间 - 实例 - 高防IP

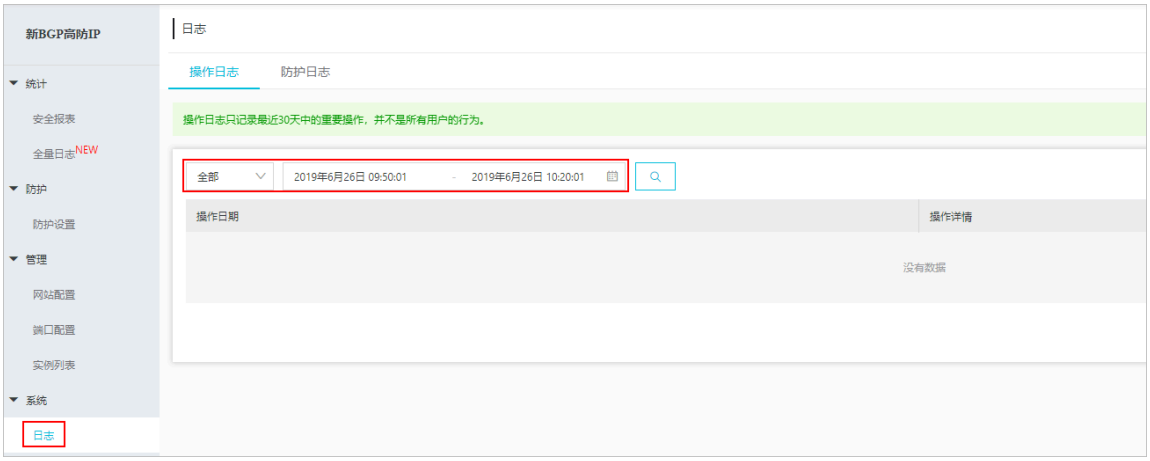
报表类型	支持查看的信息	支持的筛选项
CC攻击防护	- QPS图（攻击QPS、总QPS） - CC攻击记录	- 时间 - 被防护域名

更多信息，请参见#unique_33。

- 查询和分析日志

  在左侧导航栏，单击系统 > 日志；在日志页面，根据页签选择要查看的日志类型：操作日志、防护日志，查看对应日志记录。其中，

  - 操作日志记录最近30天中的重要操作，如IP、抗D包、ECS实例操作等，支持通过时间筛选记录。
  - 防护日志记录每个实例上发生的攻击防护事件，支持通过时间筛选记录。



如果您希望对新BGP高防的日志内容进行实时分析和报表展示，推荐您开通新BGP高防全量日志服务。开通全量日志服务后，阿里云日志服务将对接新BGP高防IP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。

新BGP高防全量日志服务是增值服务，需要单独开通并启用。要使用全量日志服务，您需要完成以下任务：

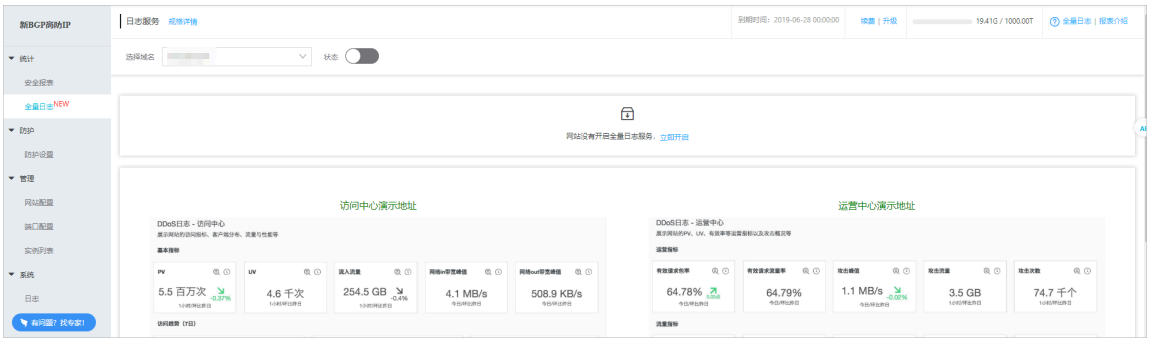
a. 开通全量日志服务，具体操作请参见*#unique_35/unique_35_Connect_42_section_tsj_h3f_g30*。

b. 启用全量日志功能，具体操作请参见*#unique_35/unique_35_Connect_42_section_brn_bn3_kgb*。

开通并启用全量日志功能后，您可以在统计 > 全量日志页面，对采集到的日志数据进行实时查询与分析、查看或编辑仪表盘、设置监控告警等。

说明:

关于全量日志中记录并支持操作的字段，请参见**全量日志字段说明**。



3.2 防护非网站业务

3.2.1 概览

本文将指导您在开通新BGP高防IP后，快速部署和使用新BGP高防，为您的非网站业务（如端游、手游、APP等）配置DDoS防护，并将业务切入新BGP高防。

使用新BGP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：添加端口配置	在新BGP高防IP控制台配置端口转发规则；然后，使用新BGP高防IP作为您的业务IP，实现业务切入。
步骤2：配置转发策略	添加端口转发规则后，您可以为其配置转发策略，具体包括：会话保持、健康检查、DDoS防护策略。
步骤3：查看业务流量	非网站业务接入新BGP高防后，您可以在新BGP高防IP控制台查看业务的流量转发数据。

3.2.2 步骤1：添加端口配置

要使用新BGP高防IP防护您的非网站业务（如端游、手游、APP等），您需要在购买新BGP高防IP实例后，配置端口转发规则，然后切换新BGP高防IP作为您的业务IP，实现业务接入。本文介绍了在新BGP高防IP控制台配置端口转发规则的具体操作。

前提条件

已开通新BGP高防IP实例。已开通的实例可以在新BGP高防IP控制台，管理 > 实例列表中查看。关于如何开通服务，请参见购买新BGP高防IP。

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。新BGP高防不会解析七层报文的内容，也不提供基于七层报文的防护（如CC攻击、Web攻击等），只支持四层防护（如SYN Flood、UDP Flood等）。在接入非网站业务时，您无需额外启用实例或选择高防节点，直接配置转发规则将非网站业务接入新BGP高防IP实例进行防护即可。

注意:

根据工信部要求，为了防止未通过备案的域名业务接入防护，新BGP高防IP不支持添加纯网络四层80端口的配置接入；为了防止私自搭建DNS防护服务器，不支持添加纯网络四层53端口的配置接入。

关于转发规则冲突

若您已经使用新BGP高防IP实例接入网站防护，则网站配置添加成功后（具体操作请参见步骤1：添加网站配置），系统将自动在您所选择的新BGP高防IP实例中为该网站域名生成相应的转发规则，该网站的流量将根据这条转发规则进行转发。

- 如果网站域名设置的转发端口为80，则系统自动生成一条转发协议为TCP、转发端口为80的转发规则。如果该转发规则已经由其它网站域名配置自动生成，则不会再次生成新的转发规则。
- 如果网站域名设置的转发端口为443，则系统自动生成一条转发协议为TCP、转发端口为443的转发规则。如果该转发规则已经由其它网站域名配置自动生成，则不会再次生成新的转发规则。

通过网站配置自动生成的转发规则无法编辑和删除（您只能编辑或删除手动添加的转发规则）。只有当使用该转发规则的所有网站域名配置取消与该新BGP高防IP实例的关联（即所有网站域名配置均不通过该新BGP高防IP实例进行防护），相关的转发规则才会被自动删除。

注意：

同一新BGP高防IP实例，同一转发协议下，每条转发规则的转发端口必须唯一。假设实例下已有通过网站配置自动生成的规则（例如，TCP协议-转发端口80或443规则），则在尝试添加同协议-同转发端口规则时，系统将提示转发规则冲突。

操作步骤

1. 登录云盾新BGP高防IP控制台。
2. 在左侧导航栏，单击管理 > 端口配置。
3. 在端口配置页面，选择要配置的新BGP高防IP实例，单击添加规则。

4. 在添加规则对话框，根据您的实际业务情况，完成规则配置。配置描述见下表。

配置项	说明
转发协议	指定源站使用的转发协议类型：TCP、UDP。
转发端口	指定新BGP高防IP实例使用的转发端口。 **说明：** 为了便于管理，一般建议转发端口与源站端口保持一致。
源站端口	指定源站使用的业务端口。

配置项	说明
源站IP	指定源站的IP。 **说明:** 支持设置多个源站IP以实现自动负载均衡；最多可配置20个源站IP。

5. 单击完成，为指定的业务创建相应转发规则。

   转发规则创建完成后，您可以根据需要配置会话保持、健康检查、DDoS防护策略。具体操作请参见步骤2：配置转发策略。

   您也可以对手动创建的转发规则执行编辑或删除操作。

6. 将实际业务IP替换为所配置的新BGP高防IP实例的IP，正式将业务流量切换至新BGP高防IP实例。

   强烈建议您在正式切换业务前进行验证，确认转发规则配置已生效。关于转发规则配置的验证方法，请参见转发规则配置生效测试。

   注意:
   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。

3.2.3 步骤2：配置转发策略

添加端口转发规则后，您可以为其配置转发策略，具体包括：会话保持、健康检查、DDoS防护策略。

前提条件

已添加端口转发规则。具体操作请参见步骤1：添加端口配置。

背景信息

通过配置转发策略，您可以根据业务实际需求，优化转发功能。例如，

- 开启基于IP地址的会话保持后，可以将来自同一IP地址的请求转发到同一个后端服务器上。
- 开启健康检查后，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。
- DDoS防护策略是基于IP地址和端口级别的防护，支持对接入新BGP高防IP的非网站业务的IP及端口的连接速度、包长度等参数进行限制，实现缓解小流量的连接型攻击的防护功能。

操作步骤

1. 登录云盾新BGP高防IP控制台。
2. 在左侧导航栏，单击管理 > 端口配置。
3. 在端口配置页面，选择要配置的新BGP高防IP实例。

4. 定位到要配置的转发规则，根据需要为其配置会话保持、健康检查、DDoS防护策略。

- 会话保持

a. 单击会话保持列下的配置。

b. 在会话保持对话框，根据需要启用或关闭会话保持：

- 如果要启用会话保持，请设置超时时间，并单击完成。
- 如果要关闭会话保持，直接单击关闭会话保持。

- 健康检查

a. 单击健康检查列下的配置。

b. 在健康检查对话框中，完成健康检查配置。配置描述见下表（单击高级设置可以展开或隐藏高级设置选项）。

类型	健康检查配置项	说明
四层、七层	检查端口	健康检查服务访问后端服务器时的探测端口。默认使用源站端口，范围为1~65535。
仅七层	域名、检查路径	仅适用于TCP协议规则。七层健康检查默认由高防转发系统向该服务器应用配置的缺省首页发起HTTP HEAD请求。 - 如果您用来进行健康检查的页面并不是应用服务器的缺省首页，则需要指定域名和具体的检查路径。 - 如果您对HTTP HEAD请求限定了host字段的参数，您只需要指定检查路径，即用于健康检查页面文件的URI。域名不用填写，默认为后端服务器的IP。

类型	健康检查配置项	说明
高级设置	响应超时时间	每次健康检查的最大超时时间，取值范围为1~30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。
高级设置	检查间隔	进行健康检查的时间间隔，取值范围为1~30秒。高防集群内所有节点，都会独立、并行地遵循该属性对后端服务器进行健康检查。由于各高防节点的检查时间并不同步，所以，如果从后端某一服务器上进行单独统计，会发现来自高防IP的健康检查请求在时间上没有遵循指定的时间间隔。
高级设置	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，取值范围为1~10。

类型	健康检查配置项	说明
高级设置	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后，状态判定为成功，取值范围为1~10。

c. 单击完成。成功开启健康检查。若您想关闭健康检查，单击配置后，直接在健康检查对话框中单击关闭健康检查即可。

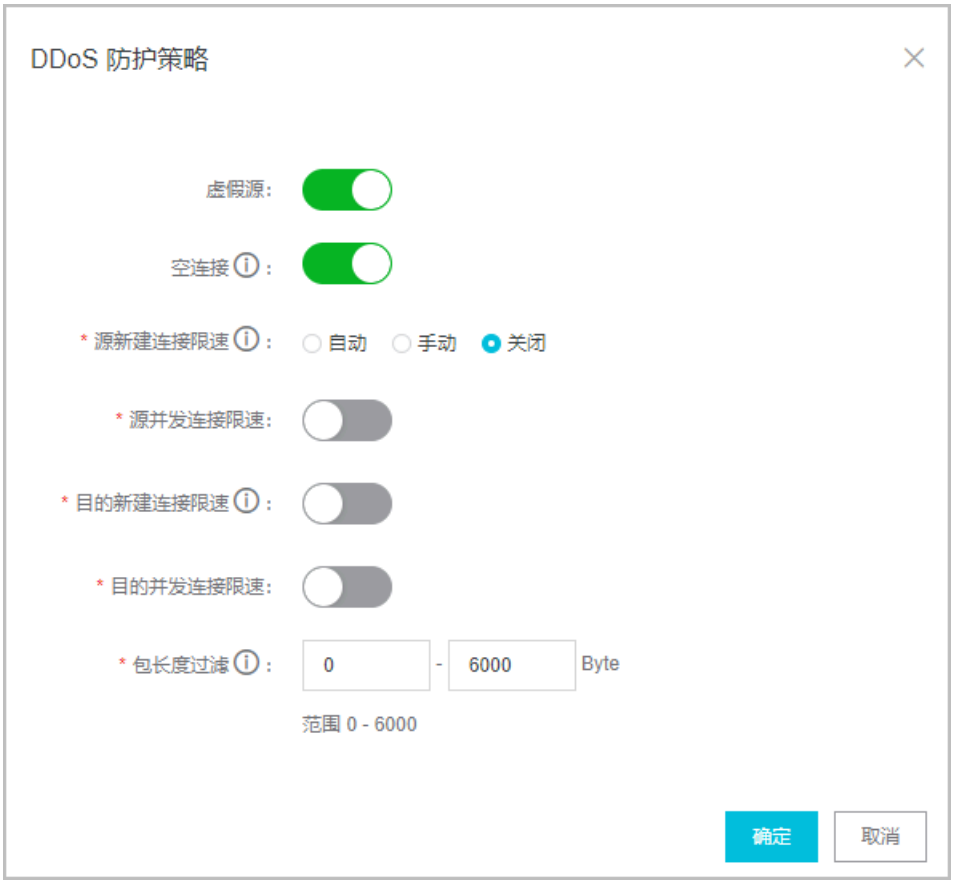
- DDoS防护策略

a. 单击DDoS防护策略列下的配置。

b. 在DDoS防护策略对话框中，完成DDoS防护策略配置。配置描述见下表。

DDoS防护策略配置项	说明
虚假源	虚假源防护，仅适用于TCP协议规则。
空连接	空连接防护，仅适用于TCP协议规则。 说明: 虚假源关闭的情况下，空连接无法开启。
源新建连接限速	单一源IP每秒新建连接数，超过限制的新建连接将被丢弃。由于防护设备为集群化部署，新建连接限速存在一定误差。支持自动或手动设置限速值，取值范围为1~50000。
源并发连接限速	单一源IP并发连接数，超过限制的并发连接将被丢弃。启用后，手动设置限速值，取值范围为1~50000。
目的新建连接限速	目的IP及端口每秒最大新建连接数，超过限制的新建连接将被丢弃。由于防护设备为集群化部署，新建连接限速存在一定误差。启用后，手动设置限速值，取值范围100~100000。
目的并发连接限速	目的IP及端口最大并发连接数，超过限制的连接将被丢弃。启用后，手动设置限速值，取值范围1000~1000000。

DDoS防护策略配置项	说明
包长度过滤	报文所含payload长度大小，单位为字节（Byte），小于最小长度或大于最大长度的包会被丢弃，取值范围为0~6000。



c. 单击确定。

3.2.4 步骤3：查看业务流量

非网站业务接入新BGP高防后，您可以在新BGP高防IP控制台查看业务的流量转发数据。

前提条件

已添加端口配置。具体操作请参见步骤1：添加端口配置。

操作步骤

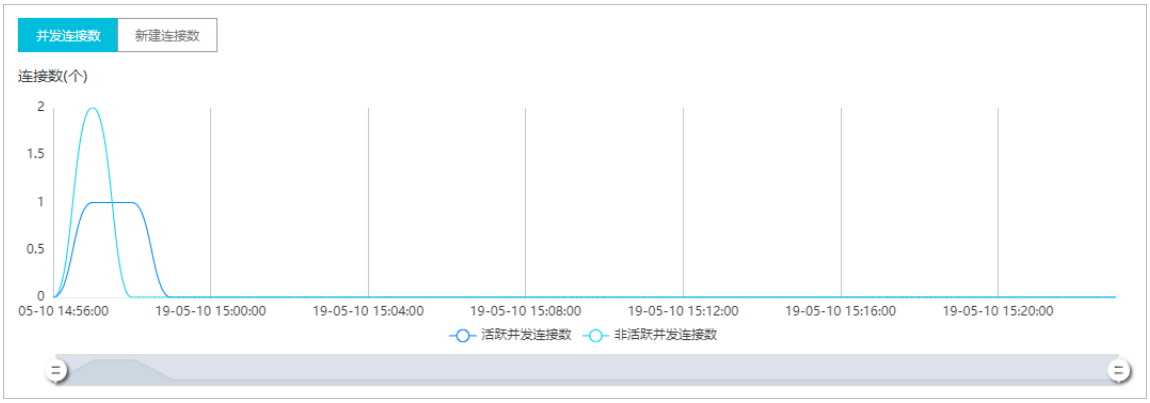
1. 登录云盾新BGP高防IP控制台。
2. 在左侧导航栏，选择管理 > 端口配置。
3. 在端口配置页面，选择要查看高防IP实例。

4. 定位到要查看的转发规则，单击其转发端口列下的跳转图标。

5. 在报表页面，业务页签下，设置查询时间（30分钟、昨天、7天、30天、近30天内自定义）后，查看指定时间段的业务流量数据。支持查看的信息包括以下内容：

- in/out带宽趋势：入带宽和出带宽曲线图、峰值、平均值

- 连接数：并发连接数和新建连接数曲线图



4 用户指南

4.1 接入设置

4.1.1 自定义非标端口

新BGP高防标准功能套餐规格的实例针对网站业务默认支持HTTP（80、8080）和HTTPS（443、8443）标准端口的DDoS攻击防护。增强功能套餐实例支持更多的HTTP、HTTPS业务非标准端口，且对被防护域名使用的不同端口的总数有相应限制。

> **说明:**
> **为网站配置添加HTTP、HTTPS非标端口，请确认您的网站域名已关联增强功能套餐规格的新BGP高防实例。**

端口总数限制

针对每个新BGP高防增强功能规格的实例，由该实例防护的全部域名所使用的不同端口的总数最多为10个。

支持的端口

> **说明:**
> **新BGP高防实例仅对所支持的HTTP、HTTPS端口提供防护。对于不支持的端口，DDoS高防既不会提供防护，也不会转发流量。例如，4444端口的业务流量到达DDoS高防实例后，将被直接丢弃。**

- **新BGP高防增强功能规格实例，针对HTTP和WebSocket协议支持以下端口：**

  80, 83, 84, 88, 89, 800, 808, 1000, 1090, 3333, 3501, 3601, 5000, 5222, 6001, 6666, 7000, 7001, 7002, 7003, 7004, 7005, 7006, 7009, 7010, 7011, 7012, 7013, 7014, 7015, 7016, 7018, 7019, 7020, 7021, 7022, 7023, 7024, 7025, 7026, 7060, 7070, 7081, 7082, 7083, 7088, 7097, 7777, 7800, 8000, 8001, 8002, 8003, 8008, 8009, 8020, 8021, 8022, 8025, 8026, 8077, 8078, 8080, 8081, 8082, 8083, 8084, 8085, 8086, 8087, 8088, 8089, 8090, 8091, 8106, 8181, 8334, 8336, 8800, 8686, 8787, 8888, 8889, 8999, 9000, 9001, 9002, 9003, 9080, 9200, 9999, 10000, 10001, 10080, 12601, 86, 9021, 9023, 9027, 9037, 9081, 9082, 9201, 9205, 9207, 9208, 9209, 9210, 9211, 9212, 9213, 48800, 87, 97, 7510, 9180, 9898, 9908, 9916, 9918, 9919, 9928, 9929, 9939, 28080, 33702

- 新BGP高防增强功能规格实例，针对HTTPS和WebSockets协议支持以下端口：

  443, 4443, 5443, 6443, 7443, 8443, 9443, 8553, 8663, 9553, 9663, 18980

4.1.2 NS方式接入网站业务

在接入新BGP高防时，您首先要完成网站配置，然后必须通过修改域名DNS，将业务流量牵引到新BGP高防实例。DNS配置支持NS接入（自动修改DNS）和手动修改两种方式。本文介绍了使用NS接入的操作方法。

前提条件

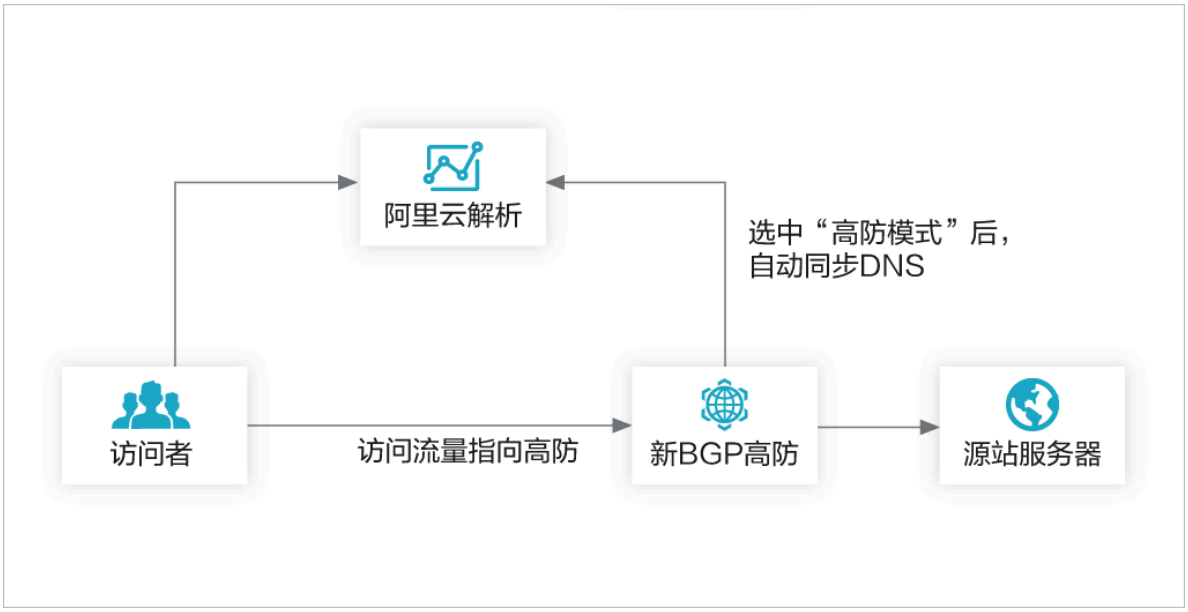
您的域名使用收费版阿里云解析DNS提供的DNS服务。如果您未开通阿里云解析DNS付费版本，则无法使用NS方式。建议先开通阿里云解析DNS付费版服务，再进行配置。

背景信息

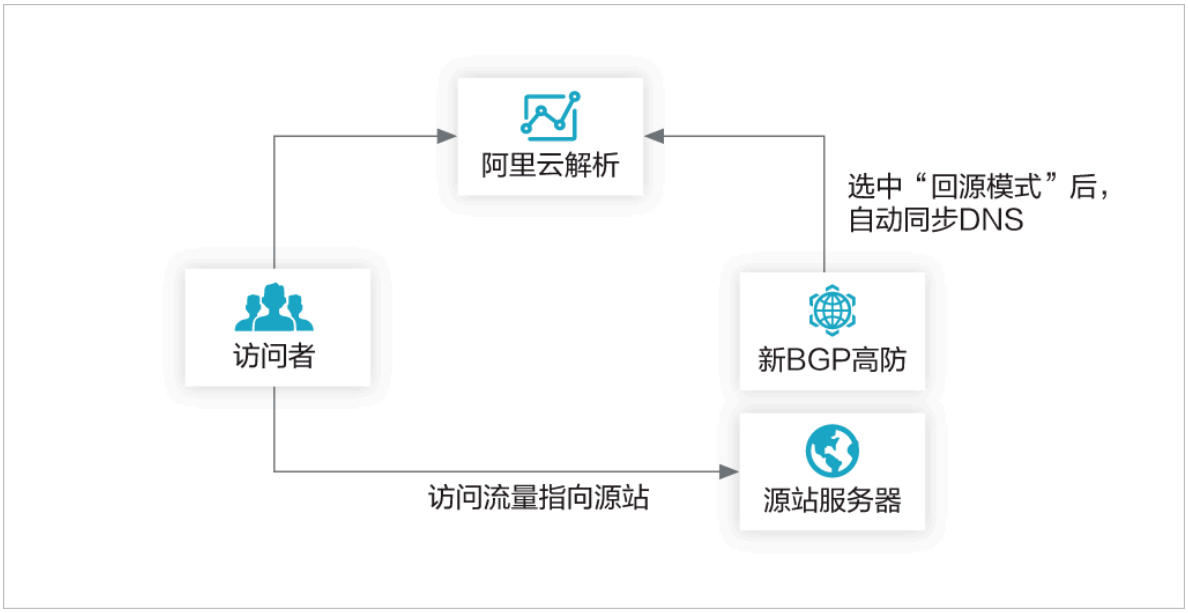
Name Server（NS）记录是指域名服务器记录，用于指定该域名由哪个DNS服务器来进行解析。

使用NS接入时，支持两种接入模式：高防和回源。

- 高防模式：将自动修改DNS记录，实现将业务流量牵引到新BGP高防上。



- 回源模式：将自动修改DNS记录，实现将业务流量指回源站。



推荐您参照本文操作步骤使用NS方式接入，方便操作。如果因特殊情况无法使用NS方式（如不具备阿里云解析DNS服务），请通过手动方式来修改DNS，将待防护业务流量牵引到新BGP高防实例。

手动修改DNS需要您通过域名的DNS服务商或DNS服务页面手动修改DNS，更新解析A记录的值为新BGP高防IP地址，从而将业务流量牵引到新BGP高防实例上。

操作步骤

1. 登录新BGP高防云盾管理控制台。
2. 定位到管理 > 网站配置页面。
3. 选择要操作的域名，单击DNS设置。

4. 开启NS方式接入。

说明:

如果当前不具有阿里云解析DNS收费版服务，将提示无法使用NS方式；如果已具有阿里云解析DNS收费版服务，开关将正常开启。

5. 根据需要选择接入模式：高防、回源。
   - 选择高防模式，新BGP控制台将自动同步阿里云解析DNS服务，将该域名的解析目标指向新BGP高防。
   - 选择回源模式，新BGP控制台将自动同步阿里云解析DNS服务，将该域名的解析目标指向源站。
6. 完成配置后，您可以通过第三方DNS测试平台来检测该域名当前最新解析结果是否符合预期。

4.1.3 上传HTTPS证书

要使新BGP高防IP帮助您清洗HTTPS业务流量，您必须在网站配置中勾选HTTPS协议，并上传HTTPS证书。已上传证书发生变化时，您也要在新BGP高防IP控制台及时更新证书。

前提条件

- 已添加网站配置（具体操作请参考步骤1：添加网站配置）且网站支持HTTPS协议。
- 准备证书文件内容。

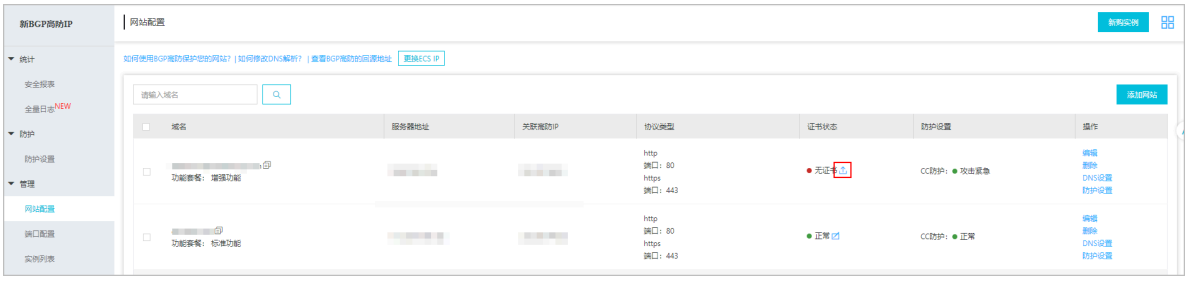
  如果您已将证书文件上传到云盾SSL证书服务进行统一管理，那么在上传证书时您可以直接选择已有证书；否则您需要准备好网站的证书和私钥文件，以完成上传操作。一般情况下，您需要准备的证书相关内容包括：

  - *.crt（公钥文件）或者*.pem（证书文件）
  - *.key（私钥文件）

操作步骤

1. 登录云盾新BGP高防IP控制台。
2. 在左侧导航栏，单击管理 > 网站配置。

3. 在网站配置列表中，定位到要操作的域名，单击其证书状态列下的上传图标。



4. 在上传证书和私钥对话框中，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以下两种：

   - （推荐）选择已有证书

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

     即使您的证书未托管在SSL证书中，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，请参考*#unique_45*。

   - 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文本框中。

     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，并复制其中的文本内容；对于其他格式（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，请参考*HTTPS证书转换成PEM格式*。

- 如果该HTTPS证书有多个证书文件（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文本框中。

证书文件文本内容样例

```
-----BEGIN CERTIFICATE-----
xxxxxxxxxxxxvs6MTXcJSfN9Z7rZ9fmxWr2BFN2XbahgnsSXM48ixZJ4krc+1M+
j2kcubVpsE2cgHdj4v8H6jUz9Ji4mr7vMNS6dXv8PUkl/qoDeNGCNdyTS5NIL5ir
+g92cL8IGOkjgvhlqt9vc65Cgb4mL+n5+DV9uOyTZTW/MojmlgfUekC2xiXa54nx
Jf17Y1TADGSbyJbsC0Q9nIrHsPl8YKkvRWvIAqYxXZ7wRwWWmv4TMxFhWRiN
Y7yZIo2ZUhl02SIDNggIEeg==
-----END CERTIFICATE-----
```

私钥文件文本内容样例

```
-----BEGIN RSA PRIVATE KEY-----
xxxxxxxxxxxxtZ3UKHJTRgNQmioPQn2bqdKHop+B/dn/4VZL7Jt8zSDGM9sTMThL
yvsmLQKBgQCr+ujntC1kN6pGBj2Fw2l/EA/W3rYEce2tyhjgmG7rZ+A/jVE9fld5sQ
ra6ZdwBcQJaiygoIYoaMF2EjRwc0qwHaluq0C15f6ujSoHh2e+D5zdmkTg/
3NKNjqNv6xA2gYpinVDzFdZ9Zujxvuh9o4Vqf0YF8bv5UK5G04RtKadOw==
-----END RSA PRIVATE KEY-----
```

5. 单击确定。

预期结果

成功上传证书后，证书状态会更新为有证书。

4.1.4 自定义TLS安全策略

新BGP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选择合适的TLS协议。

前提条件

- 网站配置已关联增强功能套餐的新BGP高防实例。
- 已添加网站配置（具体操作请参见步骤1：添加网站配置）且网站支持HTTPS协议。
- 已上传对应的HTTPS证书（具体操作请参见上传HTTPS证书）。

背景信息

如果您的业务需要通过PCI DSS 3.2认证，需要禁用TLS1.0协议；同时，您的另一个业务的访问终端仅支持TLS1.0协议，需要兼容TLS1.0协议。这种情况，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。

观看以下视频，快速了解如何在新BGP高防中自定义TLS协议版本和加密套件。

操作步骤

1. 登录云盾新BGP高防IP控制台。
2. 在左侧导航栏，单击管理 > 网站配置。
3. 选择已添加的网站业务配置，单击其证书状态列中的TLS安全策略。

4. 在TLS安全策略配置对话框中，选择TLS版本和加密套件。

- TLS版本：默认为支持TLS1.0及以上版本，兼容性最好，安全性较低。您可以根据安全需要选择仅支持TLS1.1或TLS1.2以上版本。
- 加密套件：
  - 仅支持强加密套件，安全性较高，兼容性较低

    仅支持以下强加密套件：

    ■ ECDHE-ECDSA-AES256-GCM-SHA384
    ■ ECDHE-RSA-AES256-GCM-SHA384
    ■ ECDHE-ECDSA-AES128-GCM-SHA256
    ■ ECDHE-RSA-AES128-GCM-SHA256
    ■ ECDHE-ECDSA-WITH-CHACHA20-POLY1305
    ■ ECDHE-RSA-WITH-CHACHA20-POLY1305
    ■ ECDHE-RSA-AES256-CBC-SHA
    ■ ECDHE-RSA-AES128-CBC-SHA
    ■ ECDHE-ECDSA-AES256-CBC-SHA
    ■ ECDHE-ECDSA-AES128-CBC-SHA
  - 全部加密套件，安全性较低，兼容性较高

    除上述强加密套件外，还支持以下四种弱加密套件：

    ■ RSA-AES256-CBC-SHA
    ■ RSA-AES128-CBC-SHA
    ■ ECDHE-RSA-3DES-EDE-CBC-SHA
    ■ RSA-3DES-EDE-CBC-SHA

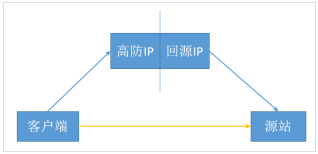
4.2 放行新BGP高防回源IP

为网站启用新BGP高防服务时，为了避免新BGP高防的回源流量被源站服务器上的安全软件误拦截，建议您设置放行新BGP高防回源IP。

背景信息

网站成功接入新BGP高防IP后，所有网站访问请求将先流转到新BGP高防，经新BGP高防IP实例清洗后再返回到源站服务器。流量经新BGP高防IP实例返回源站的过程称为回源。

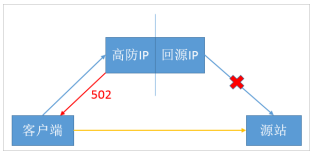
新BGP高防作为一个反向代理，其中包含了一个Full NAT的架构。



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

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

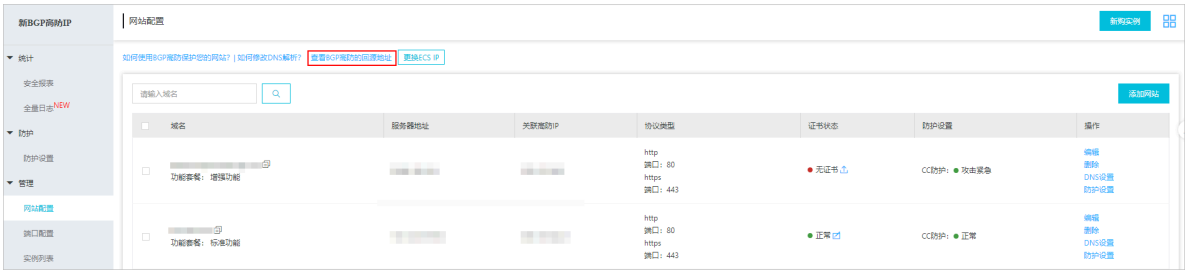
例如，最常见的502错误，即表示高防IP转发请求到源站，但源站却没有响应（因为回源IP可能被源站的防火墙拦截）。



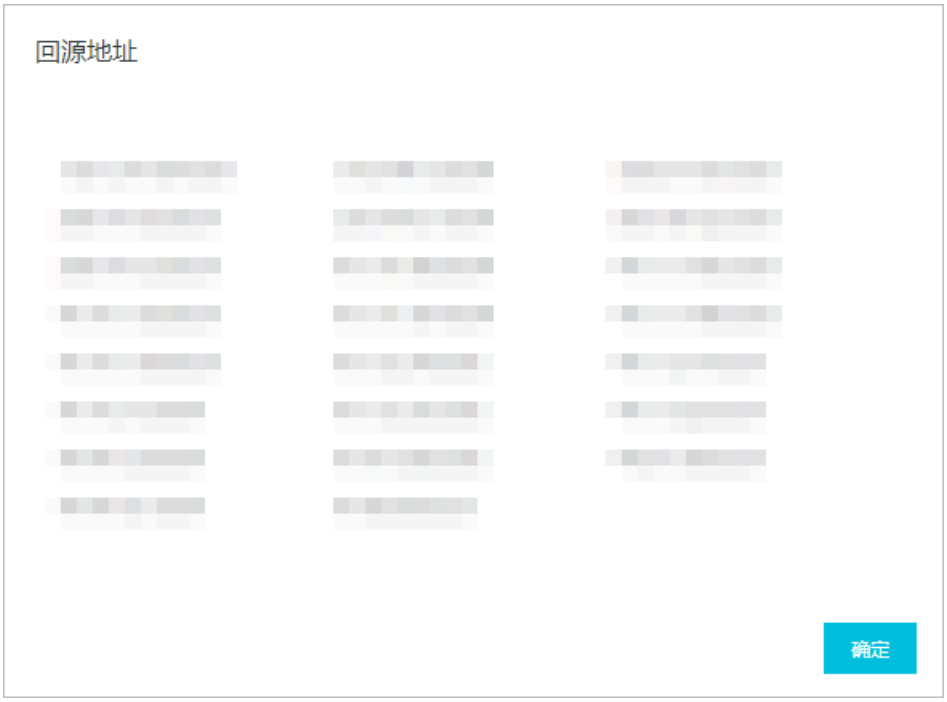
所以，在配置完转发规则后，强烈建议您关闭源站上的防火墙和其他任何安全类软件（如安全狗等），确保高防的回源IP不受源站本身安全策略的影响；或者请参见以下操作步骤，在源站服务器的安全软件中设置放行新BGP高防的回源IP地址。同时，建议您参考高防源站保护通过安全组或白名单功能为您的源站配置保护措施。

操作步骤

1. **登录云盾新BGP高防IP控制台。**
2. **在左侧导航栏，单击管理 > 网站配置。**
3. **在网站配置页面上方，单击查看BGP高防的回源地址。**



4. **在回源地址对话框中，查看并复制新BGP高防的回源地址。**



5. **打开源站服务器上的安全软件，将复制的IP段添加到白名单。**

4.3 管理实例标签

新BGP高防提供标签管理功能，方便您标记DDoS高防实例资源，实现分类批量管理。

背景信息

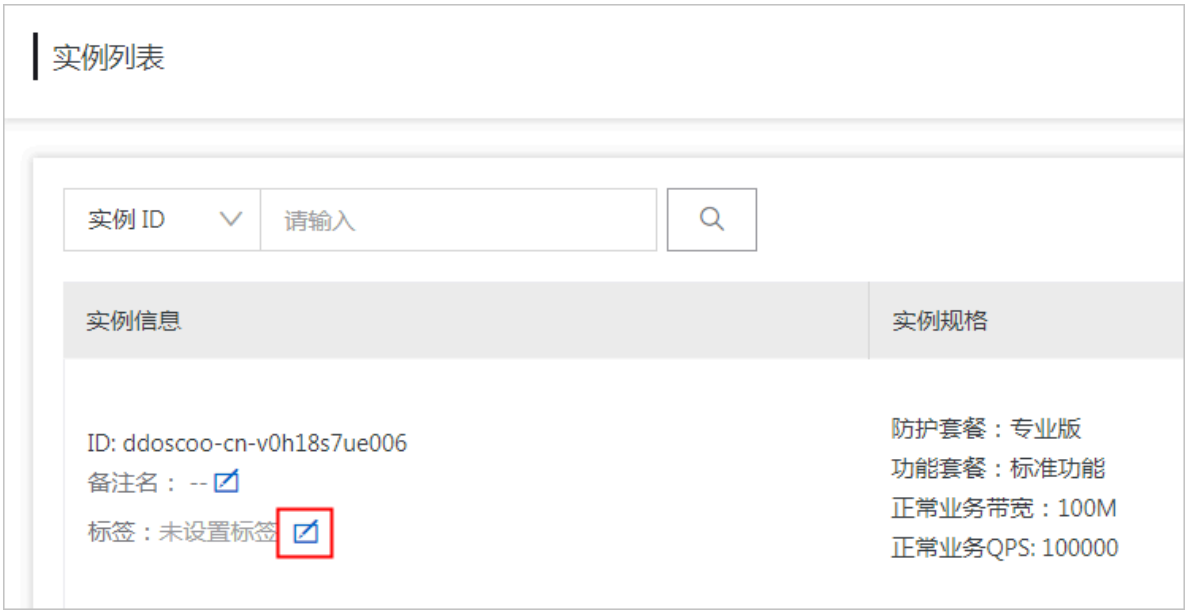
每个标签都由一对键值对（Key-Value）组成，新BGP高防实例标签存在以下使用限制：

- **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

参考以下操作步骤，为DDoS高防实例添加标签：

1. **登录新*BGP*高防控制台。**
2. **定位到管理 > 实例列表页面，选择目标高防实例。**
3. **单击实例信息列中的编辑标签按钮。**



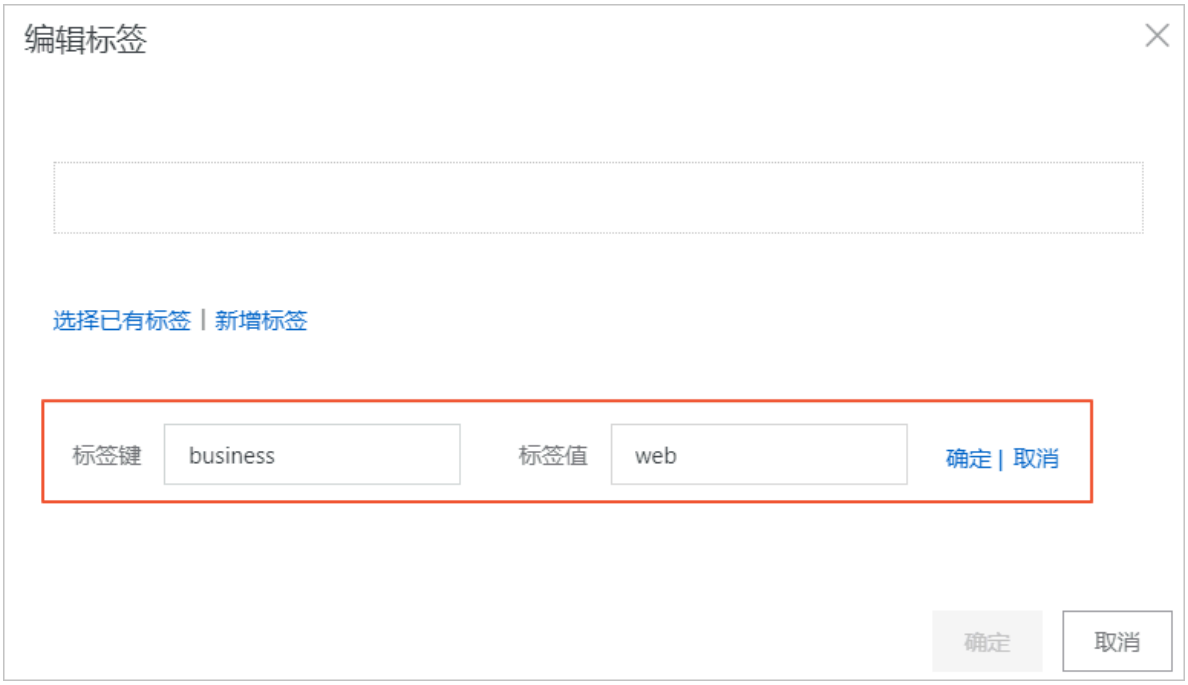
4. **在编辑标签对话框中，单击新增标签。**

> **说明:**
> **如果您已设置过标签，可以单击选择已有标签，为目标实例添加已设置的标签。**

5. **填写标签键和标签值，单击确定。**

> **说明:**

如果您选择添加已设置的标签，在列表中直接选择标签即可。



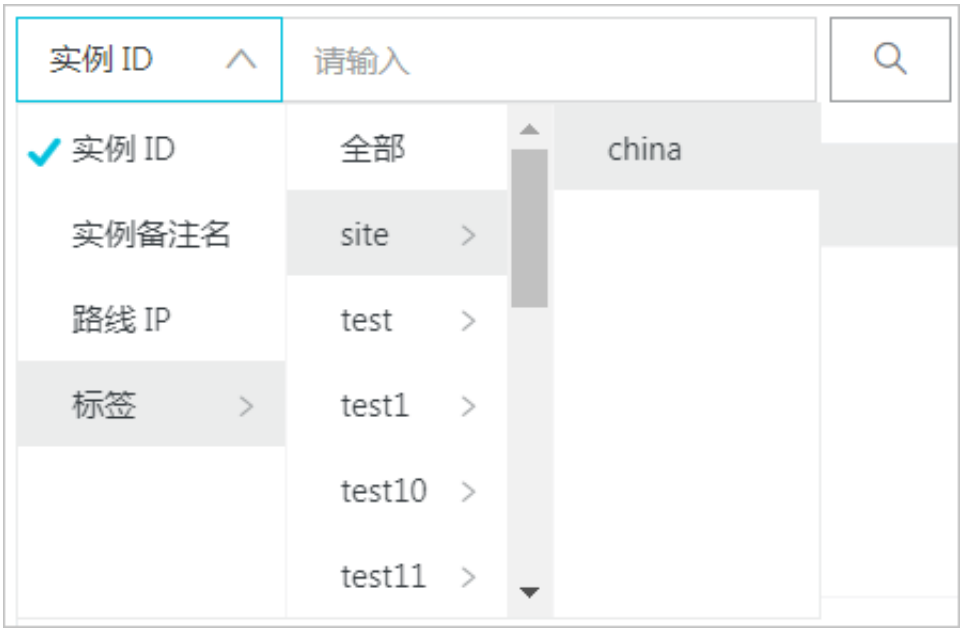
6. 单击确定，即为目标实例添加新增的标签。您可以在编辑标签对话框中为目标添加多个标签。

通过标签搜索实例

参考以下操作步骤，搜索拥有指定标签的DDoS高防实例：

1. 登录新*BGP*高防控制台。

2. 定位到管理 > 实例列表页面，单击搜索项，在下拉列表中依此选择标签、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

新BGP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。

参考以下操作步骤，删除指定DDoS高防实例的标签：

1. 登录新BGP高防控制台。
2. 定位到管理 > 实例列表页面，选择目标高防实例。
3. 单击实例信息列中的编辑标签按钮。
4. 在编辑标签对话框，单击要移除的标签的删除图标，然后单击确定。

> 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。

4.4 网络四层防护设置

4.4.1 设置DDoS防护策略

新BGP高防IP提供针对网络四层DDoS攻击的防护策略设置功能，适用于非网站业务的DDoS防护策略优化调整。

背景信息

新BGP高防IP的非网站业务的DDoS防护策略是基于IP地址+端口级别的防护，对于已接入新BGP高防IP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。

新BGP高防IP为已接入的非网站业务提供以下DDoS防护策略配置项供您选择：

> 说明：
> 新BGP高防IP的源新建连接限速防护策略配置项提供自动防护功能。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。如果选择手动模式，则需要手动设置源新建连接限速阈值。

DDoS防护策略配置项	说明
虚假源	虚假源防护，仅适用于TCP协议规则。
空连接	空连接防护，仅适用于TCP协议规则。
源新建连接限速	单一源IP每秒新建连接，超过限制的新建连接将被丢弃。由于防护设备为集群化部署，新建连接限速存在一定误差。

DDoS防护策略配置项	说明
源并发连接限速	单一源IP并发连接数，超过限制的并发连接将被丢弃。
目的新建连接限速	目的IP及端口每秒最大新建连接数，超过限制的新建连接将被丢弃。由于防护设备为集群化部署，新建连接限速存在一定误差。
目的并发连接限速	目的IP及端口最大并发连接数，超过限制的链接将被丢弃。
包长度过滤	报文所含payload长度大小，单位为字节(byte)，小于最小长度或大于最大长度的包会被丢弃。

针对非网站业务，您可以针对指定IP的指定端口设置DDoS防护策略。

说明:

DDoS防护策略配置针对端口级别生效。

操作步骤

1. 登录新*BGP*高防云盾管理控制台。
2. 定位到管理 > 端口配置页面，选择新BGP高防IP实例，选择已配置的转发规则，单击DDoS防护策略项中的配置。

3. 在DDoS防护策略对话框中，为选定的IP和端口配置DDoS防护策略。

4.4.2 设置健康检查规则

新BGP高防IP为已接入防护的端口配置提供健康检查功能。

新BGP高防IP的端口配置接入方式为业务提供基于IP地址+端口级别的防护，对于已接入新BGP高防IP实例的IP和端口提供健康检查功能。

您可以针对指定IP的指定端口设置健康检查规则。

操作步骤

1. 登录新BGP高防云盾管理控制台。
2. 定位到管理 > 端口配置页面。
3. 选择新BGP高防IP实例。

4. 选择已添加的转发规则，单击其健康检查列中的配置，配置健康检查规则。

说明:

健康检查功能默认关闭。当所选择的转发规则的转发协议为TCP协议时，您可以选择四层健康检查或七层健康检查方式。

配置项说明

说明:

配置健康检查规则的高级设置参数时，一般情况建议您使用默认值。

表 4-1: 四层健康检查

健康检查配置	说明
检查端口	健康检查服务访问后端服务器时的探测端口。默认值为配置监听时指定的后端端口。
高级设置	
响应超时时间	每次健康检查相应的最大超时时间。如果后端服务器在指定的时间内没有正确响应，则判定为健康检查失败。

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

表 4-2: 七层健康检查

健康检查配置	说明
域名和检查路径（仅限HTTP协议）	七层健康检查默认由高防转发系统向该服务器应用配置的缺省首页发起HTTP HEAD请求。 · 如果您用来进行健康检查的页面并不是应用服务器的缺省首页，需要指定域名和具体的检查路径。 · 如果您对HTTP HEAD请求限定了host字段的参数，您只需要指定检查路径，即用于健康检查页面文件的URI。域名不用填写，默认为后端服务器的IP。
检查端口	健康检查服务访问后端服务器时的探测端口。默认值为配置监听时指定的后端端口。
高级设置	
响应超时时间	每次健康检查相应的最大超时时间。如果后端服务器在指定的时间内没有正确响应，则判定为健康检查失败。
检查间隔	进行健康检查的时间间隔。高防集群内所有节点，都会独立、并行地遵循该属性对后端服务器进行健康检查。由于各高防节点的检查时间并不同步，所以，如果从后端某一服务器上进行单独统计，会发现来自高防IP的健康检查请求在时间上没有遵循指定的时间间隔。
不健康阈值	同一高防节点服务器针对同一后端服务器，在健康检查状态为成功时，连续多少次健康检查失败后，状态判定为失败。
健康阈值	同一高防节点服务器针对同一后端服务器，在健康检查状态为失败时，连续多少次健康检查成功，状态判定为成功。

4.4.3 设置会话保持规则

新BGP高防IP为已接入防护的端口配置提供会话保持功能，支持在指定时间范围内将来自同一IP地址的请求转发至同一台后端服务器。

背景信息

新BGP高防IP的端口配置接入方式为业务提供基于IP地址+端口级别的防护，对于已接入新BGP高防IP实例的IP和端口提供会话保持功能。

操作步骤

1. 登录新BGP高防云盾管理控制台。
2. 定位到管理 > 端口配置页面。
3. 选择实例并选择高防IP。
4. 选择已添加的转发规则，单击其会话保持列中的配置。

> **说明:**
> 会话保持配置针对端口级别。

5. 在会话保持对话框中，设置超时时间后，单击保存。

> **说明:**
> 如果您希望关闭会话保持功能，单击关闭会话保持即可。

4.4.4 设置流量智能防御模式

新BGP高防IP服务提供四层网络流量智能防御功能，针对网络四层DDoS攻击提供三种智能防御模式供您选择。智能防御模式调整后在数分钟内即可生效。

三种智能防御模式如下：

- 宽松：结合您的历史业务流量及阿里云攻防安全专家的经验，对来自带有明显攻击特征的恶意IP的流量进行自动清洗（算法将智能识别这些恶意IP并添加至IP黑名单进行过滤）。该模式可能无法拦截所有四层流量攻击，但误杀率低。
- 正常：结合您的历史业务流量及阿里云攻防安全专家的经验，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。该模式充分平衡防护效果和误杀率，建议您在一般情况下选择该智能防御模式。
- 严格：结合您的历史业务流量及阿里云攻防安全专家的经验，对当前正在发生的攻击行为具有最强防御效果，但可能存在一定误杀情况。

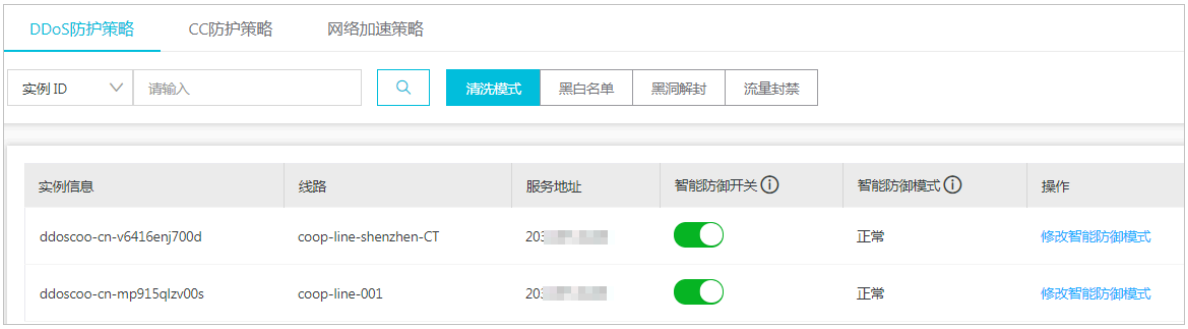
系统默认选用正常防御模式。由于智能防御功能通过算法学习您的历史业务流量情况，因此业务初次接入新BGP高防IP进行防护，系统需要三天左右时间完成对您业务流量的学习和训练，从而达到最佳防御效果。

对于智能防御算法标记的恶意IP，您可以随时查看或删除IP黑名单中的这些IP，也可以在IP黑名单中手动添加其它恶意IP进行过滤、防御。同时，您还可以将特定的IP添加至白名单，系统将直接放行来自这些IP的业务访问流量。

调整智能防御模式

默认情况下，您所购买的新BGP高防IP实例自动开启智能防御功能，并选用正常防御模式。您可以根据实际情况自由调整智能防御模式。

1. 登录新BGP高防云盾管理控制台。
2. 定位到防护 > 防护设置 > DDoS防护策略 > 清洗模式页签，选择需要调整智能防御模式的新BGP高防IP实例，单击修改智能防御模式。



说明:

智能防御模式默认开启，您可以单击智能防御开关手动关闭该功能。

3. 根据攻击情况，灵活调整智能防御模式，单击确定。

说明:

智能防御模式调整后在数分钟内即可生效。

管理黑白名单

对于智能防御算法标记的恶意IP，您可以随时查看并管理黑名单中的这些IP。同时，您还可以将特定的IP添加至白名单，系统将直接放行来自这些IP的业务访问流量。

- **黑名单**

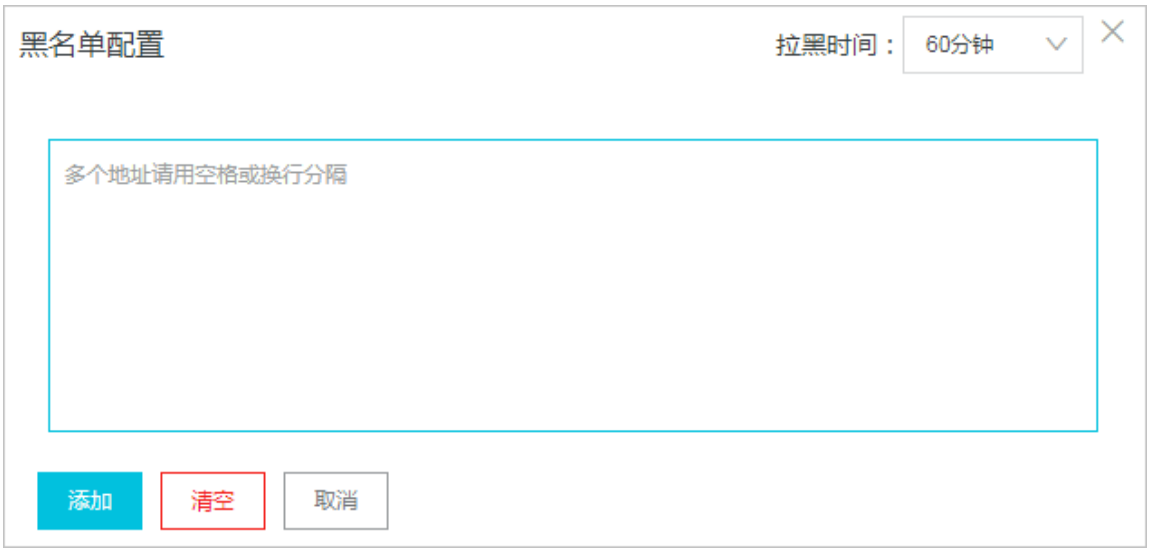
  定位到防护 > 防护设置 > DDoS防护策略 > 黑白名单页签，单击黑名单，选择新BGP高防IP实例，即可查看并管理当前被智能防护算法标记的或手工添加的IP黑名单明细情况。

  说明:

黑名单中的IP存在有效期，并非永久生效。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（如果该恶意IP在有效期间有持续的恶意攻击行为，系统将自动延长有效期）；通过手动添加的IP，在添加时需要指定其有效期。

IP黑名单支持以下操作：

- **关键字搜索：在搜索框中输入关键字，单击查询按钮即可过滤黑名单中符合条件的IP。**
- **下载：单击下载，可以将当前黑名单中的IP列表下载至本地。**
- **清空黑名单：单击清空黑名单，可以将当前黑名单中的所有IP移除。**
- **手动添加：单击手动添加，可以在黑名单中手动添加额外的IP并设置拉黑时间进行过滤。**



说明：

黑名单最多支持手动添加2000个IP。

- **白名单**

定位到防护 > 防护设置 > DDoS攻击防护 > 黑白名单页签，单击白名单，选择新BGP高防IP实例，即可管理IP白名单。

说明：

白名单中的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。即如果IP已经被添加至白名单，则无法将该IP添加至黑名单中。

IP白名单支持以下操作：

- 关键字搜索： 在搜索框中输入关键字，单击查询按钮即可过滤白名单中符合条件的IP。
- 下载： 单击下载，可以将当前白名单中的IP列表下载至本地。
- 清空白名单： 单击清空白名单，可以将当前白名单中的所有IP移除。
- 手动添加： 单击手动添加，可以在白名单中手动添加IP放行来自该IP的访问流量。

说明:

白名单最多支持添加500个IP。

4.4.5 手动解除黑洞状态

对于已加入新BGP高防防护的网站，如果因为其保底防护带宽或弹性带宽不足被突发大流量攻击造成黑洞，您可以在新BGP高防控制台使用黑洞解封来快速恢复业务。每个用户每天共拥有五次黑洞解封的机会。

背景信息

解除黑洞操作方便您在意外进入黑洞时快速恢复业务，建议您在解除黑洞前先提升保底或弹性防护能力，避免网站被持续打入黑洞。

操作步骤

1. 登录云盾新BGP高防IP控制台。
2. 定位到防护 > 防护设置页面。
3. 前往DDoS防护策略页签，并选择黑洞解封。

说明:

- 每个用户每天拥有5次黑洞解除机会，每天零点会自动恢复成5次；只有成功解除黑洞状态才会消耗1次解除额度。

- 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，则相邻两次解除操作的间隔必须大于10分钟。

4. 找到处于黑洞状态的BGP高防IP，确认平台自动解封时间（即执行解封后业务恢复的时间）后，单击其操作列下的解封，并耐心等待黑洞状态自动解除。

   - 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”，则请您耐心等待下再尝试。
   - 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新BGP高防线路是否已恢复正常。

4.4.6 主动封禁海外流量

新BGP高防服务支持对新BGP高防IP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，且在流量封禁期间可以随时解除封禁。

背景信息

当您遭遇特大流量攻击，且发现攻击流量有超过最大防护能力的趋势时，建议您考虑使用流量封禁。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，将攻击规模控制在自身最大防护能力范围内。

开启流量封禁会将特定流量在机房侧丢弃，降低新BGP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，启用流量封禁可在一定情况下降低被黑洞的概率。

操作步骤

1. 登录云盾新BGP高防IP控制台。
2. 定位到防护 > 防护设置页面。

3. 前往DDoS防护策略页签，单击流量封禁。

4. 选择需要封禁的新BGP高防IP实例的电信或联通线路，单击封禁。

说明:

- 支持分别封禁电信和联通两大运营商的海外流量，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。如果流量还是很大，超过当前防护能力，可以再考虑封禁联通海外流量。
- 每个用户总共拥有10次封禁机会，不会每天刷新封禁次数。封禁一次电信或联通海外流量都会消耗一次额度。

5. 在流量封禁对话框中，选择封禁区域（仅海外）、封禁时长，并单击确认。

说明:

每次封禁时长最短15分钟，最长23小时59分钟。

6. 完成封禁操作。

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

4.5 网络七层防护设置

4.5.1 设置网站访问黑白名单

新BGP高防IP服务支持对已接入防护的网站域名设置黑名单和白名单。

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

说明:

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

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

1. **登录云盾新*BGP*高防*IP*控制台。**
2. **定位到管理 > 网站配置页面，选择已接入防护的域名，单击防护设置。**

3. **在CC防护策略页签，定位到黑白名单区块，单击设置。**

说明:

配置黑白名单必须启用CC安全防护功能。

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

说明:

IP或IP段支持以IP或IP/掩码的格式填写，支持分别配置最多200条黑白名单记录，多条记录之间用英文“,”进行分隔。

说明:

- 黑白名单配置暂不支持非网站防护。
- 黑白名单配置完成后即刻生效。

  注意:

  在一定情况下，可能需要经过一些访问流量和时间后才会真正生效。如添加黑白名单配置后未立即生效，请尝试继续访问数次。
- 黑名单支持添加0.0.0.0/0，即拦截来自除白名单中配置的已知IP外所有IP的访问。
- 黑白名单配置后，对在该网站域名绑定的所有新BGP高防IP实例生效。

4.5.2 封禁特定区域IP访问

区域封禁帮助您一键阻断来自指定地区（中国大陆省份、港澳台特别行政区、大洲）的来源IP的所有访问请求。该功能目前只针对指定域名生效。

前提条件

使用区域封禁功能前，请确认您的网站域名已接入增强功能套餐的新BGP高防实例。

背景信息

假设example.aliyundemo.com域名的正常用户均来自中国大陆（含港澳台特别行政区），您可以为example.aliyundemo.com域名配置区域封禁，封禁来自海外地区（亚洲，欧洲，北美洲，南美洲，非洲，大洋洲，南极洲）的访问请求。

注意事项

- 区域封禁针对域名级别生效，如果您需要对多个不同网站域名进行区域封禁，则需要对不同域名分别进行设置，不支持对多个域名批量配置。
- 区域封禁根据源IP的归属区域在新BGP高防中识别过滤，并不能减小进入BGP高防网络的攻击流量。

操作步骤

1. 登录云盾新BGP高防管理控制台。
2. 定位到防护 > 防护设置 > CC防护策略。
3. 选择需要设置区域封禁的域名（以example.aliyundemo.com为例），开启区域封禁开关。

4. 在区域封禁配置页面，单击设置，选择封禁区域。以下图中的配置为例，配置生效后，海外流量将无法访问到example.aliyundemo.com。

5. 选择区域后，单击确定，配置生效。

4.5.3 设置精准访问控制规则

精准访问控制允许您设置访问控制规则，对常见的HTTP字段（如IP、URL、Referer、UA、参数等）进行条件组合，用来筛选访问请求，并对命中条件的请求设置放行、阻断、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。

背景信息

精准访问控制规则由匹配条件与匹配动作构成。在创建规则时，您通过设置匹配字段、逻辑符和相应的匹配内容定义匹配条件，并针对符合匹配条件规则的访问请求定义相应的动作。

匹配条件

匹配条件包含匹配字段、逻辑符、匹配内容。匹配内容暂时不支持通过正则表达式描述，但允许设置为空值。

匹配动作

精准访问控制规则支持以下匹配动作：

- 阻断：阻断命中匹配条件的访问请求。
- 放行：放行命中匹配条件的访问请求。
- 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。

规则匹配顺序

如果您设置了多条规则，则多条规则间有先后匹配顺序，即访问请求将根据您设定的精准访问控制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。

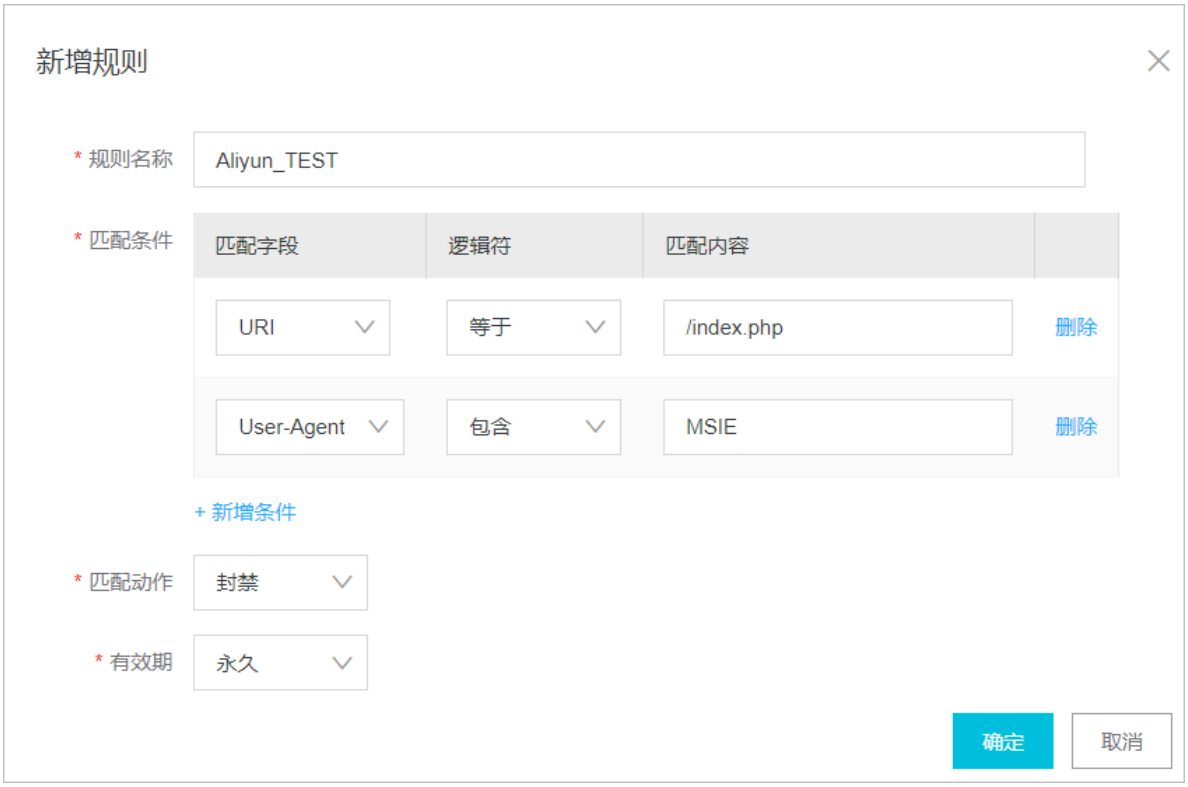
注意事项

- 精准访问控制规则存在规则数限制。
  - 标准功能套餐实例：针对每个接入防护的网站域名业务支持配置最多五条规则，且仅支持使用IP、URL、Referer、User-Agent字段作为匹配字段。
  - 增强功能套餐实例：针对每个接入防护的网站域名业务支持配置最多十条规则。
- 精准访问控制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。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。

操作步骤

1. 登录云盾新BGP高防管理控制台。
2. 定位到防护 > 防护设置 > CC防护策略。
3. 选择需要设置精准访问控制规则的域名（以example.aliyundemo.com为例），开启精准访问控制开关。

4. 在精准访问控制的操作区域，单击设置进行规则配置。以下图为例，配置完成后，对于/index.php页面，UserAgent字段中包含MSIE的请求将被拦截。



支持的匹配字段

说明:

标准功能套餐的新BGP高防实例仅支持使用IP、URL、Referer、User-Agent字段作为匹配字段。

匹配字段	字段描述	适用逻辑符
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

匹配字段	字段描述	适用逻辑符
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

匹配字段	字段描述	适用逻辑符
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
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，如GET、POST等。	· 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

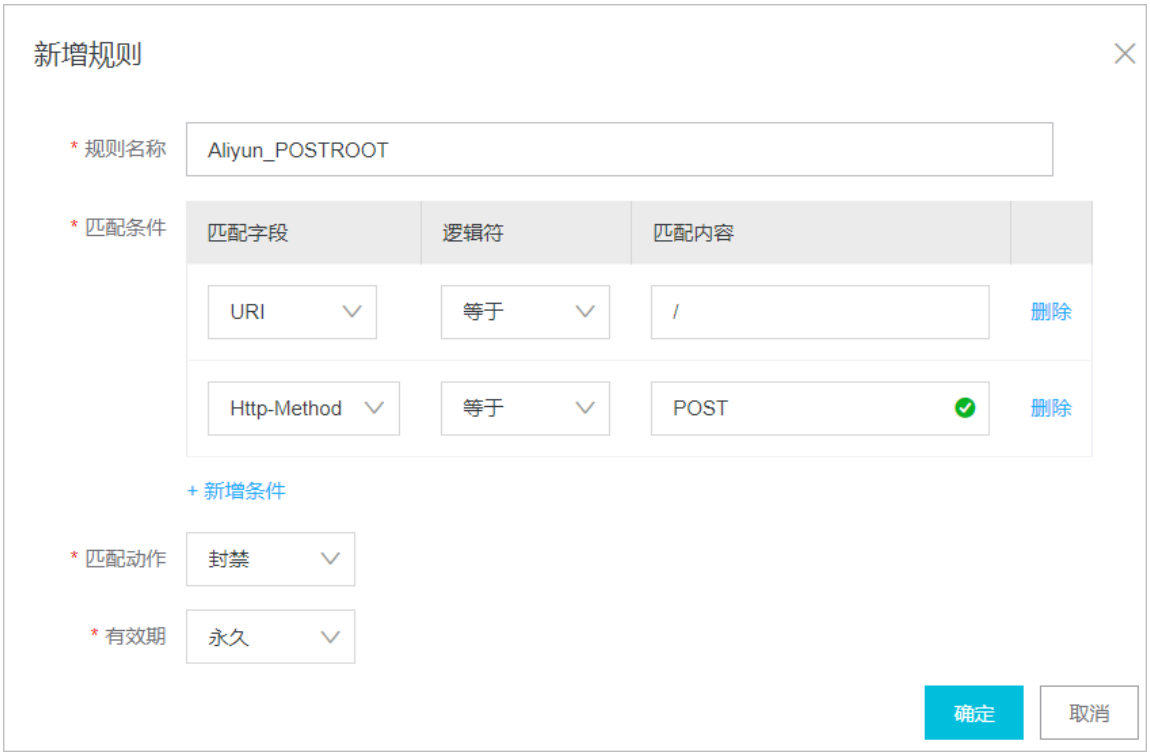
匹配字段	字段描述	适用逻辑符
params	访问请求的URL地址中的参数部分，通常指URL中”?”后面的部分。例如，www.abc.com/index.html?action=login中的action=login就是参数部分。	· 包括 · 不包括 · 等于 · 不等于 · 长度小于 · 长度等于 · 长度大于

其他配置示例

您可以参考以下精准访问控制规则的配置示例进行配置。

- **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。如果被CC攻击时，发现客户端的请求中存在大量的POST根目录请求，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，有大量爬虫请求，若不排除是攻击肉鸡模拟爬虫进行CC攻击，则可以对爬虫的请求执行拦截操作。

5. 完成配置后，单击确定，配置生效。

4.5.4 防护HTTP(S) Flood攻击

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

- 正常模式：默认的CC安全防护模式。网站无明显流量异常时建议采用此模式。

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

  攻击紧急模式的CC攻击防护策略相对严格。相比正常模式，此模式可以防护更为复杂和精巧的CC攻击，但可能会对少部分正常请求造成误杀。
- 严格模式：严格模式的CC攻击防护策略较为严格。同时，该模式会对被保护网站的所有访问请求实行全局级别的人机识别验证，即针对每个访问者进行验证，只有通过认证后访问者才允许访问网站。

> **说明:**
> 对于严格模式的全局算法认证，如果是真人通过浏览器的访问请求均可以正常响应；但如果被访问网站的业务是API或原生app应用，将无法正常响应该算法认证，导致网站业务无法正常访问。

- **超级严格模式：超级严格模式的CC攻击防护策略非常严格。同时，该模式会对被保护网站的所有访问请求实行全局级别的人机识别验证，即针对每个访问者都将进行验证，只有通过认证后后才允许访问网站。**

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

  说明:

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

操作步骤

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

1. **登录云盾新BGP高防IP控制台。**
2. **定位到管理 > 网站配置页面，选择已接入防护的网站域名配置记录，单击防护设置。**

3. **在CC防护策略页签，定位到CC安全防护区块，选择CC攻击防护模式。**

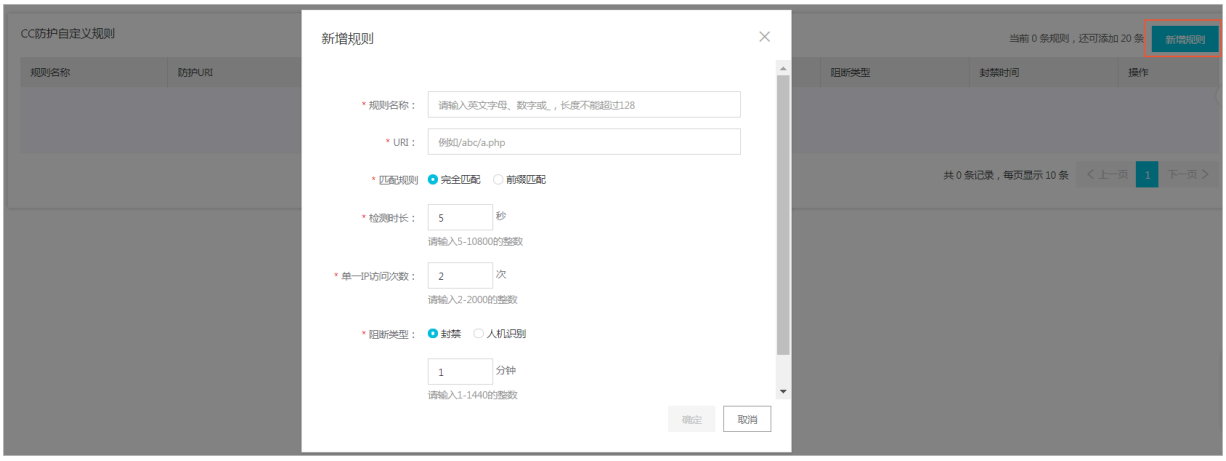
   说明:

   如果您不想使用CC安全防护功能，可以单击状态开关关闭该功能。

自定义规则

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

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



CC安全防护设置最佳实践

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

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

说明:

如果您的网站业务是API或原生app应用，由于无法正常响应严格模式中的相关算法认证，无法使用严格或超级严格模式进行防护。因此，需要通过配置CC安全防护自定义规则对被攻击的URL配置针对性的防护策略拦截攻击请求。

4.5.5 启用AI智能防护

AI智能防护基于阿里云的大数据能力，通过智能分析引擎自学习业务流量基线，动态调整防护模型，及时帮助您发现并阻断恶意攻击，例如恶意Bot、HTTP flood攻击等。

启用AI智能防护功能

1. **登录云盾新BGP高防管理控制台。**
2. **定位到防护 > 防护设置 > CC防护策略。**

3. 选择需要设置AI智能防护的域名（以example.aliyundemo.com为例），开启AI智能防护开关。

4. 选择防护模式和防护等级。

AI智能防护提供两种模式供您选择：

- 预警：仅记录日志，不进行阻断。您可以通过全量日志功能查看所记录的攻击预警日志。
- 防护：对恶意请求直接进行拦截。

> 说明：
> 建议您先使用预警模式并通过全量日志报表观察攻击日志记录，完全确认AI智能防护效果后再将防护模式设置为防护使其真实生效。

AI智能防护提供三种防护等级供您选择：

防护等级	防护效果	适用场景
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。
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情况适用。

查看智能防护规则

开启AI智能防护后，当检测到恶意攻击行为时，高防实例自动生成防护规则。您可以在精准访问控制规则模块中查看具体防护规则。

AI智能防护规则的名称以“smartcc_”开头。

> 说明：

- 开启AI智能防护后，系统自动生成的智能防护规则无法手动删除。而关闭AI智能防护后，所生成的防护规则将立即清空。
- AI智能防护预警模式时自动生成的精准防护规则其动作均是预警（只记录攻击日志，不进行拦截）。

注意：

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。

查看攻击预警日志

当检测到恶意攻击行为且命中AI智能防护的防护规则时，高防的全量日志功能中将记录相应的攻击日志。

注意：

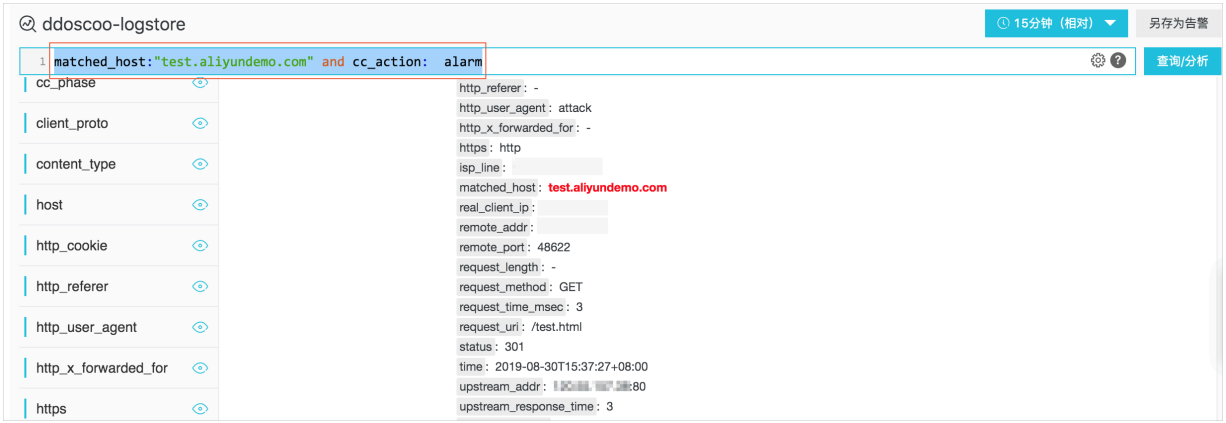
请确认您已为该域名开通全量日志功能。关于全量日志的更多信息，请参见*#unique_35*。

如果您的AI智能防护模式设置为预警时，您可以在统计 > 全量日志页面中，选择相应的域名并输入以下查询语句，查看所记录的攻击预警日志：

```
matched_host:"test.aliyundemo.com" and cc_action:alarm
```

说明：

请将`test.aliyundemo.com`替换为您需要查看的已开启AI智能防护预警模式的域名。



4.5.6 加速网站静态页面访问

新BGP高防在流量清洗中心集成网页缓存技术，在为您的网站提供DDoS防护的同时还可以加速网站静态页面的访问。

前提条件

使用静态页面缓存功能前，请确认您的网站域名已接入增强功能套餐的新BGP高防实例。

背景信息

您可以通过静态页面缓存功能加速您已接入新BGP高防的网站域名访问。同时，您可以通过自定义规则为域名中的指定页面设置缓存策略。

操作步骤

1. 登录云盾新BGP高防管理控制台。
2. 定位到防护 > 防护设置 > 网络加速策略。
3. 选择需要使用静态页面缓存功能的域名，开启静态页面缓存开关。
4. 选择静态页面缓存模式。
   - 标准：仅对该网站域名的静态文件请求（.css，.js，.txt）尝试进行缓存。
   - 增强：对该网站域名的所有请求尝试进行缓存。
   - 不缓存：不对该网站域名的请求进行缓存。

5. 您可以单击设置，为该网站域名的指定页面设置自定义规则。
   a) 单击新增规则。
   b) 在新增规则对话框中，填写指定页面的URI，选择缓存模式，并且可以设置页面缓存的过期时间。

> 说明:

页面缓存规则中的URI无需填写参数，且不支持通配符。例如，填写/a/即指定www.a.com/a/路径下的所有页面。

4.5.7 更换源站ECS公网IP

若您的源站IP已暴露，建议您更换阿里云ECS云服务器的公网IP，防止黑客绕过新BGP高防直接攻击源站。您可以在新BGP高防IP管理控制台更换后端ECS的IP，每个账号最多可更换10次。

背景信息

说明:
更换ECS IP功能仅支持使用经典网络公网IP的ECS更换IP。

操作步骤

1. 登录云盾新BGP高防IP控制台。
2. 定位到管理 > 网站配置页面。
3. 单击更换ECS IP。

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。

4. 更换ECS IP需要将ECS停机，若您已将需要更换IP的ECS停机，请直接跳转到步骤6。在更换ECS IP对话框，单击前往ECS，并在ECS管理控制台将需要更换IP的ECS实例停机。

   a) 在实例列表中找到目标ECS实例，单击其实例ID。

   b) 在实例详情页，单击停止。

   c) 选择停止方式，并单击确定。

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

   d) 等待ECS实例状态变成已停止。

5. 返回更换ECS IP对话框，输入ECS实例ID，并单击下一步。
6. 确认当前ECS实例信息准确无误（尤其是ECS IP）后，单击释放IP。
7. 成功释放原IP后，单击下一步，为该ECS实例自动分配新的IP。
8. ECS IP更换成功，单击确认，完成操作。

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

4.6 查看安全总览

在将业务接入新BGP高防IP服务并切换业务流量至新BGP高防IP实例后，您可以在新BGP高防IP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。

背景信息

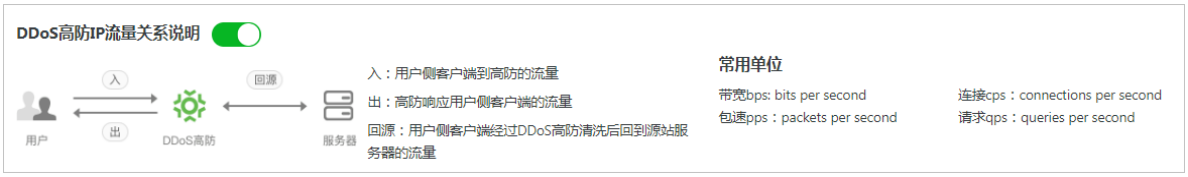
新BGP高防IP的安全总览页面向您展示以下业务指标和DDoS攻击事件的概览：

- 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。

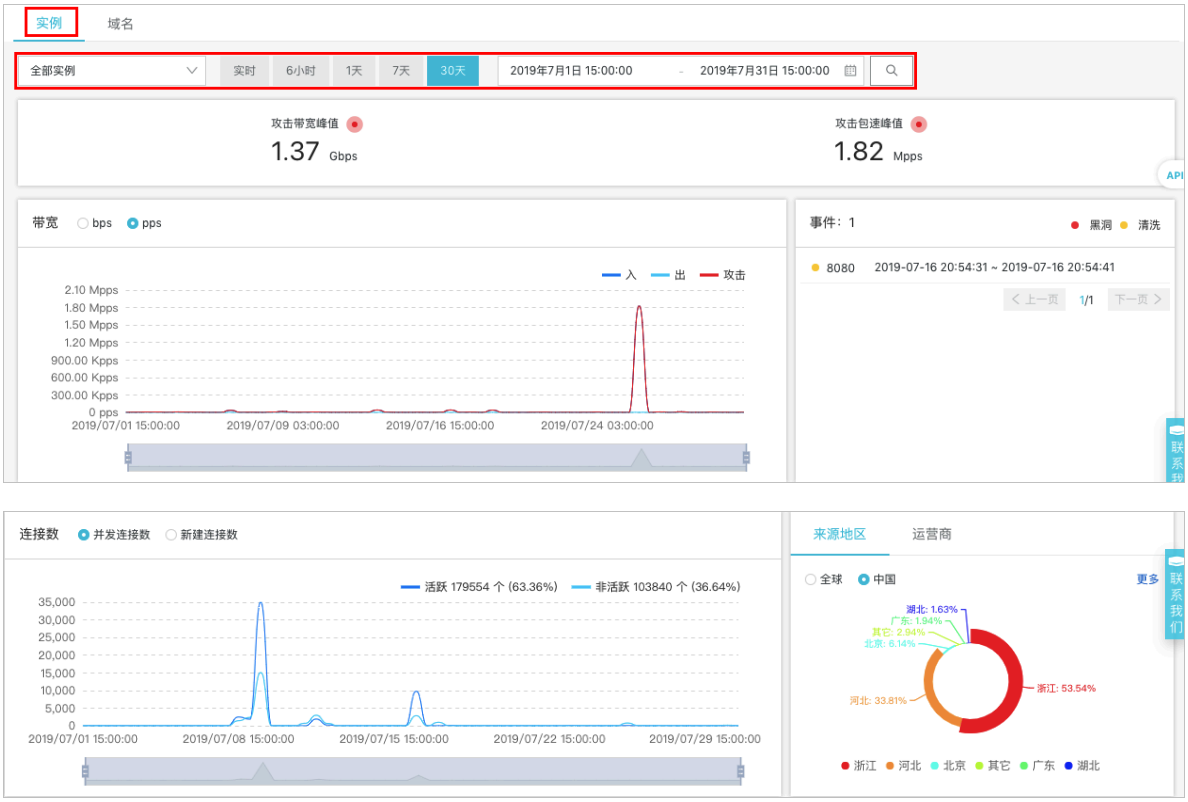
操作步骤

1. 登录云盾新BGP高防IP控制台。
2. 定位到统计 > 安全总览，查看并熟悉DDoS高防IP的背景信息及相关概念。

   安全总览展示了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。



3. 打开实例页签，设置要查询的时间范围，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。

- 攻击带宽峰值和攻击包速峰值
- 带宽趋势（入流量、攻击流量、出流量）
- （攻击）事件

  将鼠标放到被攻击的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。

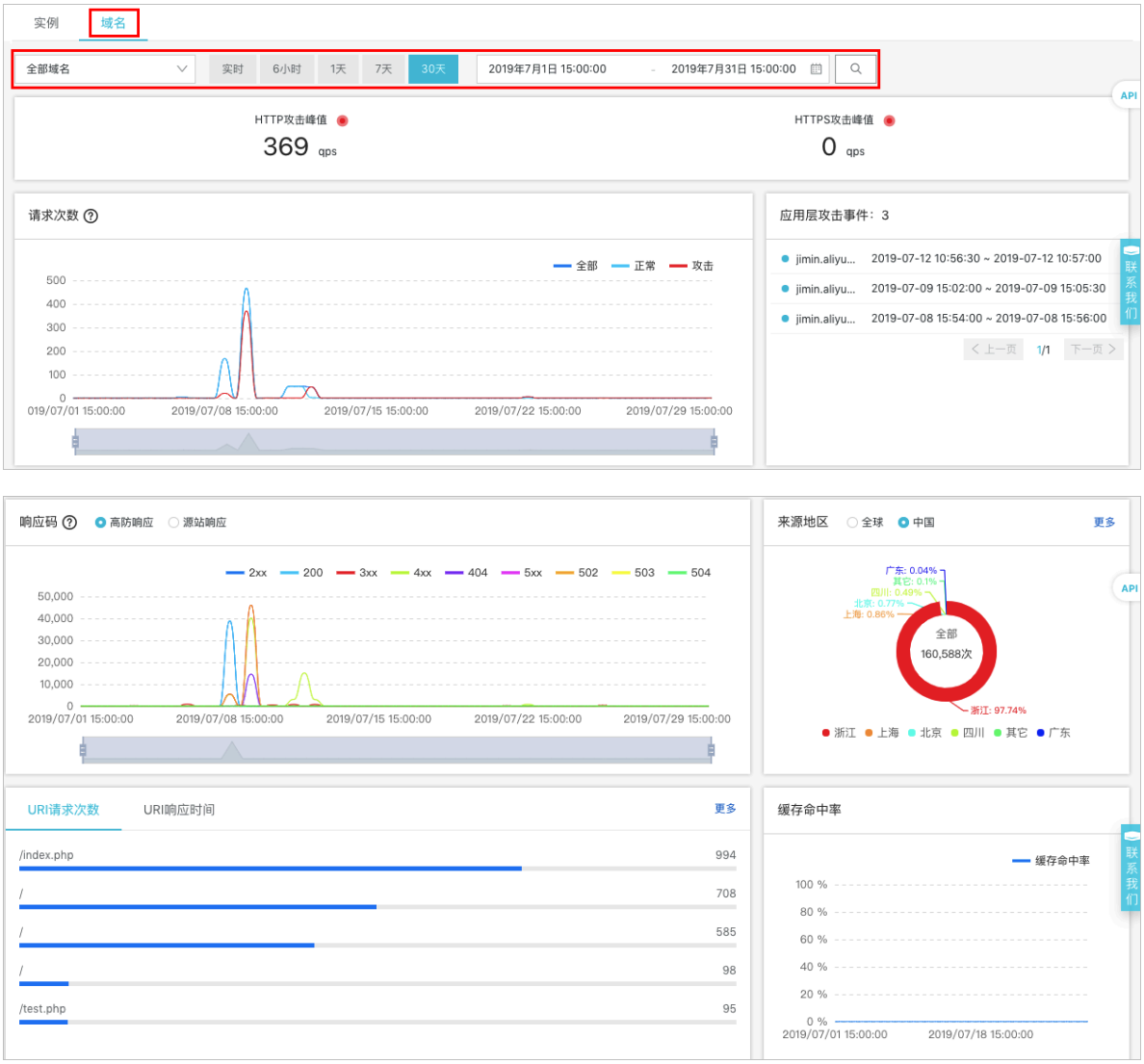
- （端口）连接数
  - 并发连接数：客户端同一时间与高防建立的TCP连接数量
  - 新建连接数：客户端每秒内新增的与高防通信的TCP连接数

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1个以上实例，则无法区别端口，只能显示全部端口的连接数。

- **访问来源区域和运营商分布**

4. 打开域名页签，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攻击峰值和HTTPS攻击峰值
- 请求次数趋势图

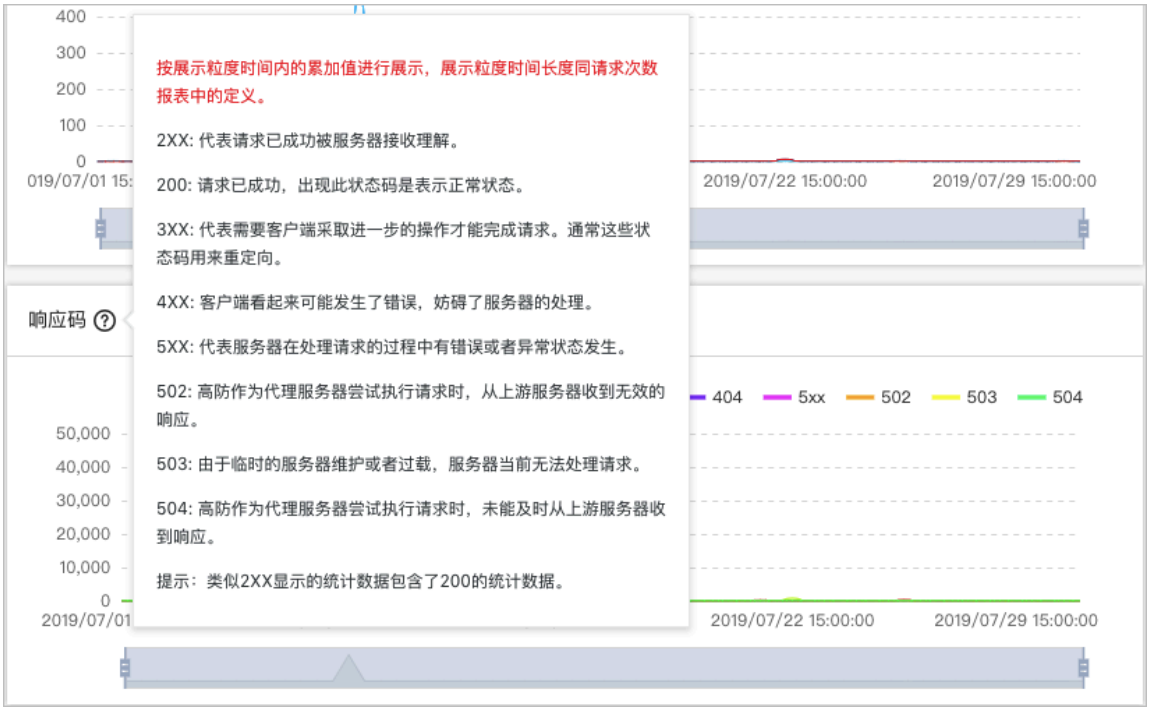
  请求次数趋势图按峰值展示，不同的查询时间间隔对应的展示粒度不同，具体如下：

  - 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30分钟；
  - 1-7天，展示粒度为1小时；
  - 7天-15天，展示粒度为4小时；
  - 其它，展示粒度为12小时。
- 应用层攻击事件

将鼠标放到被攻击的域名上，可以展示被攻击的域名信息、攻击的峰值和攻击类型。

- 响应码信息

响应码记录的数量对应展示粒度时间内的累加值，展示粒度的时间长度定义同请求次数趋势图中的定义。您可以通过响应码旁的帮助信息了解具体响应码的含义。



- 访问来源地区分布
- URI请求次数和URI响应时间记录
- 缓存命中率记录

> **说明:**
> 只有开通网站缓存加速功能，才会有缓存命中率数据。更多信息，请参见加速网站静态页面访问。

4.7 全量日志

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

背景信息

根据*APNIC 2017*年*DDoS*风险报告，超过80%的DDoS攻击都会混合HTTP攻击，而其中混合的CC攻击尤其隐蔽，因此通过日志对访问和攻击行为进行即时分析研究、附加防护策略就显得尤其重要。

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

开通全量日志服务

1. 登录新*BGP*高防*IP*管理控制台，定位到统计 > 全量日志页面，单击立即购买前往全量日志服务购买页面。
2. 根据您的业务需要，选择合适的全量日志服务规格。
   - 日志存储量：日志信息的最大存储空间，单位TB。

     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信息。建议您关注日志存储空间的使用量，及时升级日志存储量规格。
   - 使用时长：全量日志服务的有效期。

     全量日志服务有效期到期后，将停止存储新的日志信息。服务到期七天后如仍未续费延长服务有效期，将自动删除所有日志信息。

   全量日志服务的单价为500元/TB（日志存储量）/月（使用时长）。

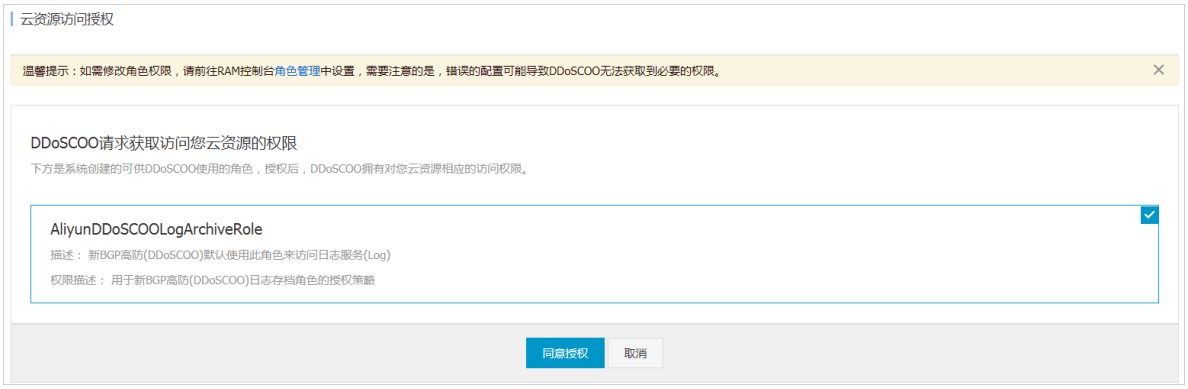
   说明:

当全量日志服务的日志存储量足够大且在服务有效期内，将从使用全量日志服务的第一天开始，连续存储180天的日志信息。第181天的日志信息，将覆盖第一天存储的日志信息，即始终保持存储最近180天的全量日志信息。

日志存储量选择参考示例

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（即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）。

3. 单击立即购买，完成支付。
4. 回到新BGP高防IP管理控制台的统计 > 全量日志页面，单击立即授权。
5. 在云资源访问授权页面中，单击同意授权，授权新BGP高防服务将日志存储至您的日志服务专属日志库中。



开通全量日志服务并完成云资源访问授权后，您可以在全量日志页面单击规格详情，查看当前的全量日志服务规格信息。

说明:

建议您在全量日志服务使用期间，定期关注全量日志存储空间的使用情况和服务有效期。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。

为网站启用全量日志

参考以下操作步骤，为您需要开启全量日志功能的网站域名启用该功能：

1. 登录新*BGP*高防*IP*管理控制台，定位到统计 > 全量日志页面。

2. 选择网站域名，单击状态开关或立即开启，为该网站域名启用全量日志功能。

启用全量日志功能后，您可以在全量日志页面对采集到的日志数据进行实时查询与分析、查看或编辑仪表盘、设置监控告警等。关于新BGP高防服务的日志分析与日志报表功能，请参见*#unique_59*和*#unique_60*。

使用全量日志功能

依托于阿里云日志服务强大的功能，为网站域名启用全量日志功能后，在全量日志页面您可以对所采集的网站访问日志和攻击防护日志进行深入的分析、以可视化的方式展示、根据所设定的阈值实现监控报警等。

功能项	说明	更多信息
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，查询和分析语句之间通过|进行分割。 例如，您可以通过以下查询分析语句查询域名的访问量： `* | SELECT COUNT(*) as times, host GROUP by host ORDER by times desc limit 100` 更多查询语句示例，请参见常用查询语句示例。	查询与分析
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。同时，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。	分析图表
仪表盘	仪表盘是日志服务提供的实时数据分析大盘。您将常用的查询语句以图表形式展示后，可将分析图表保存到仪表盘中。 同时，新BGP高防的全量日志功能默认为您提供DDoS访问中心和DDoS运营中心两个仪表盘。 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。	仪表盘
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

全量日志功能应用场景

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

- **排查网站访问异常**

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

  例如，通过以下语句查看网站访问日志：

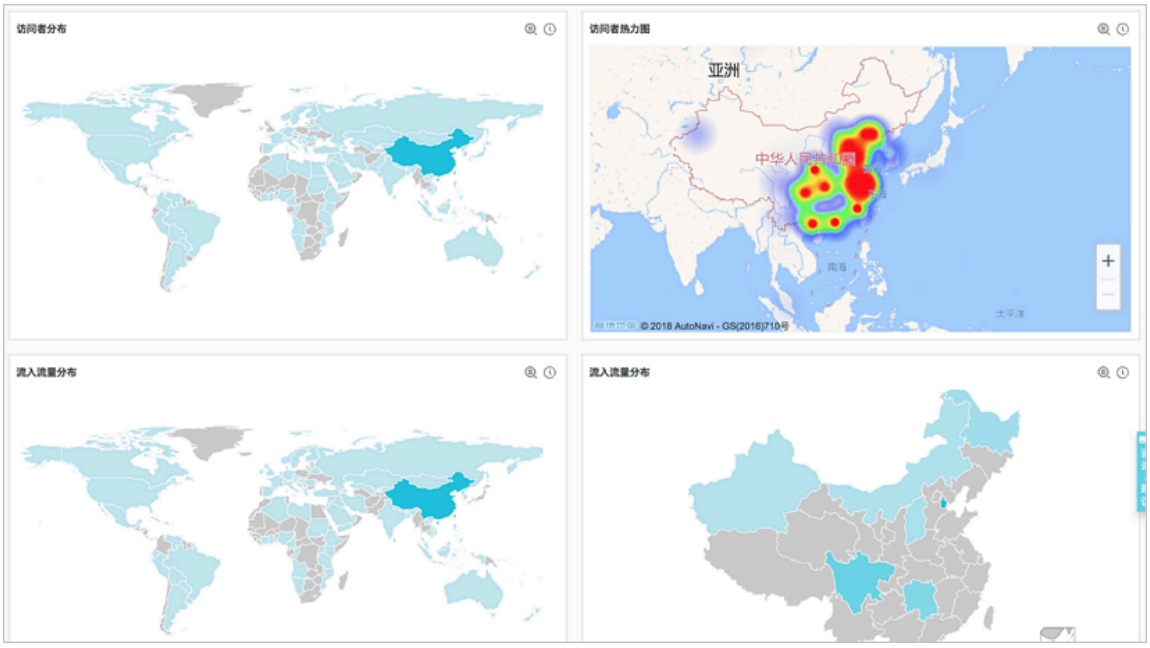
  ```
  __topic__: DDoS_access_log
  ```

- **追踪CC攻击者来源**

  访问日志中记录了CC攻击者的分布及来源，通过对DDoS访问日志进行实时查询与分析，您可以对CC攻击者进行来源追踪、溯源攻击事件，为您的应对策略提供参考。

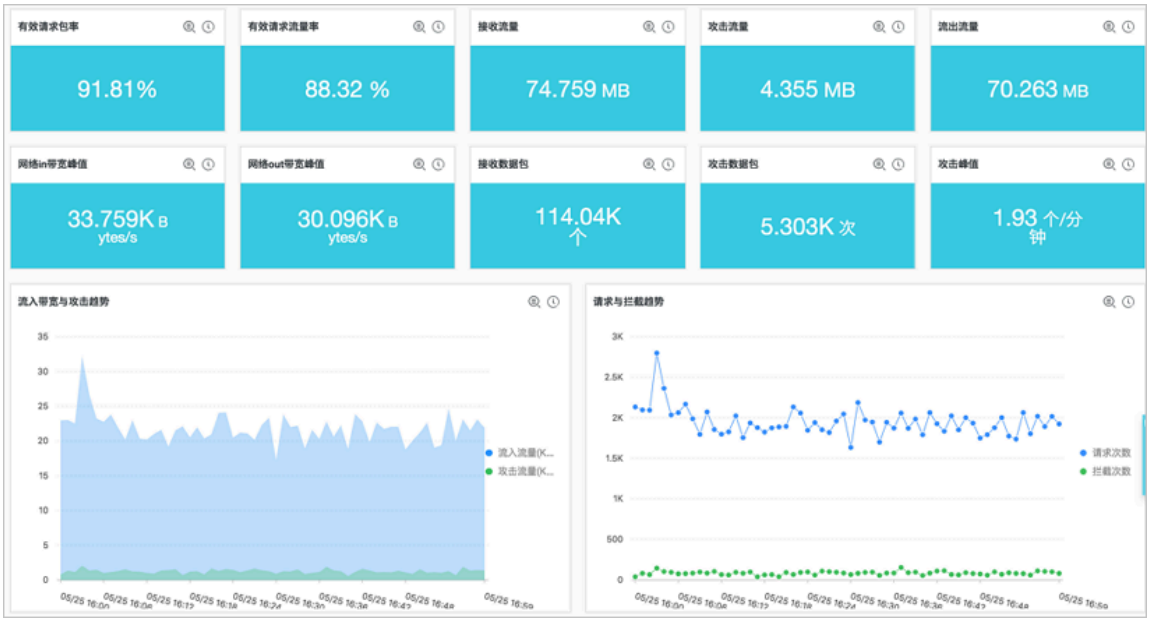
  - **例如，通过以下语句分析DDoS访问日志中记录的CC攻击者国家分布：**

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

  - **例如，通过以下语句查看访问PV：**

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

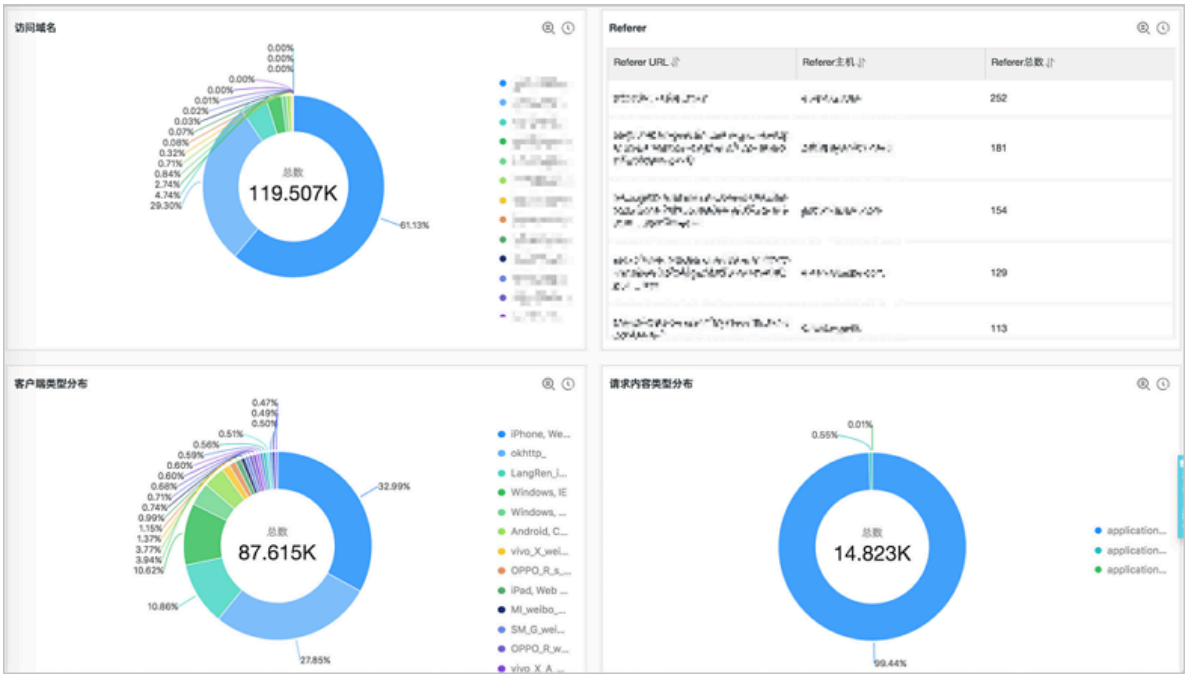
    

- **网站运营分析**

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

  例如，查看来自各个网络服务提供商的访问者流量分布：

```
__topic__: DDoS_access_log | select ip_to_provider(if(real_client_ip
='-', remote_addr, real_client_ip)) as provider, round(sum(request_le
ngth)/1024.0/1024.0, 3) as mb_in group by provider having ip_to_prov
ider(if(real_client_ip='-', remote_addr, real_client_ip)) <> '' order
by mb_in desc limit 10
```



常用查询语句示例

- **拦截类型查询**

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

- **QPS查询**

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

- **被攻击域名查询**

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

- **被攻击URL查询**

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

- **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
```

- **5XX状态码查询**

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

- **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"
```

相关文档

- **全量日志字段说明**
- **日志查询语法**
- ***SQL*分析语法**

4.8 日志查询

4.8.1 操作日志

您可以在云盾新BGP高防IP控制台的日志页面，查看近30天的重要操作日志。

说明:

操作日志只记录最近30天中的重要操作，并非记录所有用户行为。

操作日志内容	支持情况
ECS更换IP日志	支持
黑洞解封操作日志	支持
流量封禁/解封操作日志	支持
四层流量清洗模式变更操作日志	支持
CC防护模式变更操作日志	支持
弹性防护带宽变更操作日志	支持

4.8.2 全量日志字段说明

新BGP高防的全量日志功能记录丰富的日志字段。

您可以在当前的全量日志页面对采集到的日志进行实时查询与分析等操作。详细的日志字段说明，参见下表。

字段	说明	示例
__topic__	日志主题（Topic），固定为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.abc.com
http_cookie	请求cookie。	k1=v1;k2=v2
http_referer	请求referer，若没有，显示为-。	http://xyz.com
http_user_agent	请求User Agent。	Dalvik/2.1.0 (Linux; U; Android 7.0; EDI-AL10 Build/HUAWEIEDISON-AL10)
http_x_forwarded_for	通过代理跳转的上游用户IP。	-

字段	说明	示例
https	该请求是否为HTTPS请求，其中： · true：该请求是HTTPS请求。 · false：该请求是HTTP请求。	true
matched_host	匹配的配置的源站，可能是泛域名。未匹配则为-。	*.zhihu.com
real_client_ip	访问客户的真实IP，获取不到时为-。	1.2.3.4
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。	1.2.3.4
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
request_uri	请求路径。	/answers/377971214/banner
server_name	匹配到的host名，没有匹配到则为default。	api.abc.com
status	HTTP状态。	200
time	时间。	2018-05-02T16:03:59+08:00
cc_action	CC防护策略行为，例如none、challenge、pass、close、captcha、wait、login、n等。	close

字段	说明	示例
cc_blocks	表示是否被CC防护策略阻断，其中： · 1：表示阻断。 · 其他内容表示通过。 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	表示是否被CC防护策略阻断，其中： · ok：表示通过。 · failed：表示不通过，包括校验未通过和阻断。 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。 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。 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。 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。 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。 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。 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。 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`，多个地址用逗号分隔。	1.2.3.4:443
upstream_ip	实际回源地址IP。	1.2.3.4
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。	12345678
querystring	请求字符串。	token=bbcd&abc=123

4.9 业务配置批量导入导出

当您的网站域名配置或四层转发规则配置数量过多时，如果您需要保存当前时间点的业务接入配置或进行配置迁移，您可以通过业务配置的批量导入/导出功能，快速完成这类操作。

- **转发规则配置的批量导入/导出功能支持TXT文本格式。**
- **网站域名配置的批量导入/导出功能，采用兼容性更强的XML文件格式。相比于TXT文本格式，XML文件格式的参数扩展性和可读性都更强。同时，支持网站配置的源站是域名的场景的配置批量导入/导出。**

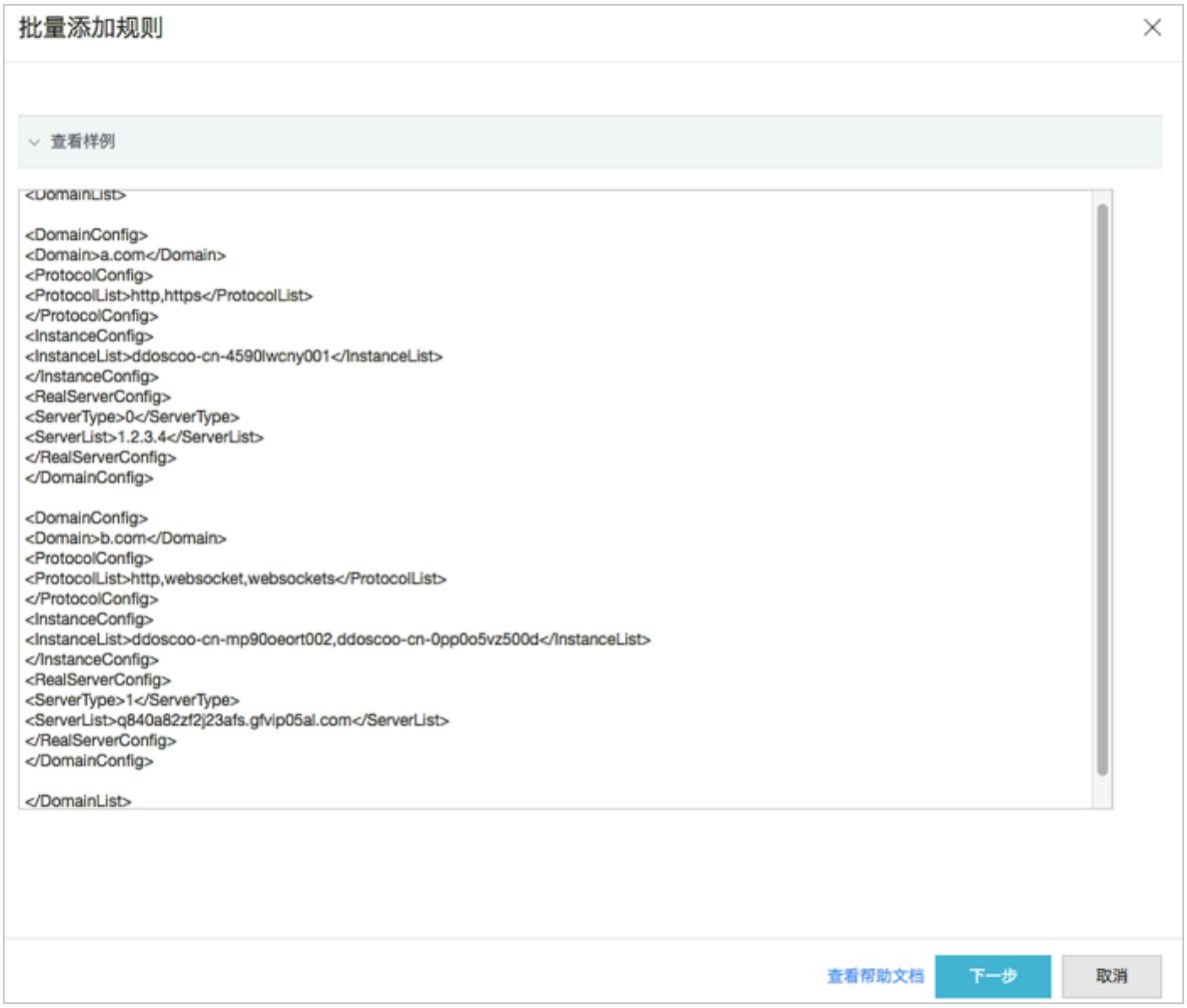
批量导入网站域名配置

1. **登录云盾新BGP高防IP控制台。**
2. **定位到管理 > 网站配置页面，在域名配置列表下方单击批量域名导入，一次性配置多个网站域名。**

3. **在批量添加规则对话框中，按照特定的XML格式输入域名配置参数内容。**

说明:

文本框支持粘贴和复制功能。



XML格式参数说明

域名配置参数内容必须以`<DomainList>`开始，`</DomainList>`结束，中间部分是待导入的域名配置参数信息。其中，每个域名的配置参数均以`<DomainConfig>`开始，`</DomainConfig>`结束，中间部分为与该域名配置相关的具体参数，详见下表。

说明:

每多添加一个域名配置，则增加一个`<DomainConfig>……</DomainConfig>`结构数据体。

域名配置具体参数	说明
`<Domain>a.com</Domain>`	指定待配置的域名（只能输入一个域名）。
`<ProtocolConfig><ProtocolList>http,https</ProtocolList></ProtocolConfig>`	指定域名协议类型。指定多个协议类型时以英文“,”隔开，本示例表示该域名的协议类型为http和https。

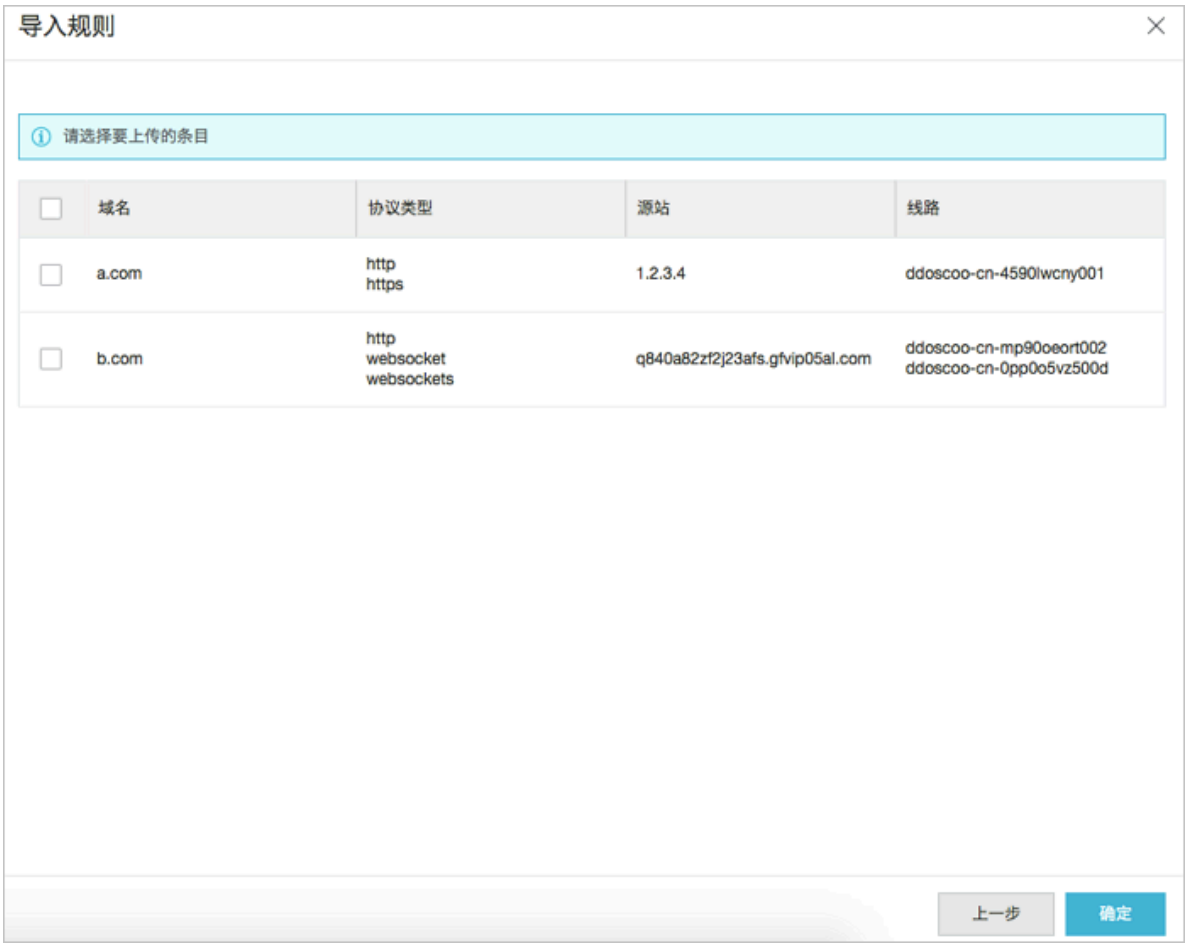
<InstanceConfig><InstanceList>ddoscoo-cn-4590lwcny001</InstanceList></InstanceConfig>	指定为该域名配置的新BGP高防IP实例。 **说明:** 由于每个新BGP高防IP实例对应一个高防IP，只需填写新BGP高防IP的实例ID即可。指定多个实例时以英文字符“,”隔开。
<RealServerConfig><ServerType>0</ServerType><ServerList>1.2.3.4</ServerList></RealServerConfig>	指定源站信息。其中， • <ServerType>0</ServerType>：表示源站IP类型 • <ServerType>1</ServerType>：表示源站域名类型 在<ServerList>1.2.3.4</ServerList>中指定源站地址，指定多个地址时以英文字符“,”隔开。 **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。

域名配置参数内容样例

```
<DomainList>
 <DomainConfig>
 <Domain>a.com</Domain>
 <ProtocolConfig>
 <ProtocolList>http,https</ProtocolList>
 </ProtocolConfig>
 <InstanceConfig>
 <InstanceList>ddoscoo-cn-4590lwcny001</InstanceList>
 </InstanceConfig>
 <RealServerConfig>
 <ServerType>0</ServerType>
 <ServerList>1.2.3.4</ServerList>
 </RealServerConfig>
 </DomainConfig>
 <DomainConfig>
 <Domain>b.com</Domain>
 <ProtocolConfig>
 <ProtocolList>http,websocket,websockets</ProtocolList>
 </ProtocolConfig>
 <InstanceConfig>
 <InstanceList>ddoscoo-cn-mp90oeort002,ddoscoo-cn-0pp0o5vz500d</
InstanceList>
 </InstanceConfig>
 <RealServerConfig>
 <ServerType>1</ServerType>
 <ServerList>q840a82zf2j23afs.gfvip05al.com</ServerList>
 </RealServerConfig>
 </DomainConfig>
```

```
</DomainList>
```

4. 单击下一步。如果XML配置参数文本内容正确，将被解析成所需导入的域名配置。



5. 勾选所需导入的域名配置信息，单击确定，即可将所选择的域名配置批量导入。

批量导出网站域名配置

1. 定位到管理 > 网站配置页面，在域名配置列表下方单击批量域名导出，单击确定，即开始执行域名配置导出任务。

2. 单击网站配置页面右上角的任务进度按钮，查看导出任务下载进度。

3. 耐心等待任务完成，在任务列表对话框单击下载，即可下载所导出的网站配置信息。

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。

批量导入转发规则配置

1. 定位到管理 > 转发规则页面，在转发规则列表下方单击批量添加，选择添加规则，一次性配置多条转发规则。

说明:

您也可以选择添加会话/健康配置或添加DDoS防护策略，批量添加相应规则配置。

2. 按照所弹出的对话框中的文件内容样例添加规则配置信息。

- 添加转发规则

- 添加会话/健康检查配置

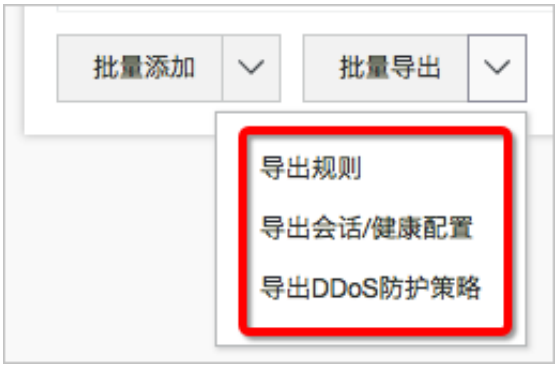
- 添加DDoS防护策略

3. **单击确定，即可将相关配置导入。**

批量导出转发规则配置

1. **定位到管理 > 转发规则页面，在转发规则列表下方单击批量导出，选择导出规则，单击确定，即可导出当前转发规则配置。**

> **说明:**
> **您也可以选择导出会话/健康配置或导出DDoS防护策略，导出相应规则配置。**



2. **单击转发规则页面右上角的任务进度按钮，查看导出任务下载进度。**
3. **耐心等待任务完成，在任务列表对话框单击下载，即可下载所导出的规则配置信息。**

> **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。**

4.10 从高防IP迁移至新BGP高防IP

背景信息

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

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

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

新BGP高防IP规格说明

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

迁移至新BGP高防IP

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

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

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

开始之前

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

1. 登录云盾DDoS高防IP管理控制台。

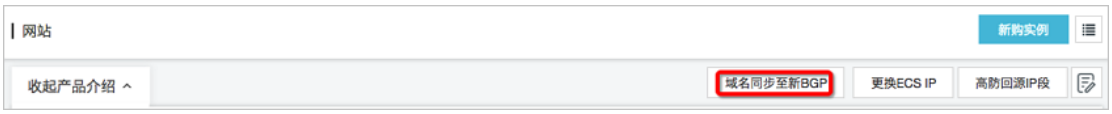
2. 将业务配置迁移至新BGP高防IP实例。

- 网站域名配置迁移

  域名配置迁移前注意事项：

  - 请勿在新BGP高防IP实例中添加80或443的端口转发配置。因为新BGP高防IP的域名配置默认占用80或443端口进行转发，如果在新BGP高防IP实例中已添加80或443端口配置，将导致所迁移的域名配置无法正常关联新BGP高防IP实例。
  - 如果您之前通过提交工单在后台开通HTTP2或HTTPS强制转HTTP回源的功能，请务必在域名同步前关闭这些功能。
  - 当所迁移的域名与其它账号的泛域名配置存在冲突时，将导致所迁移的域名配置无法正常关联新BGP高防IP实例。如果您拥有多个阿里云账号，请注意检查是否存在此类冲突。

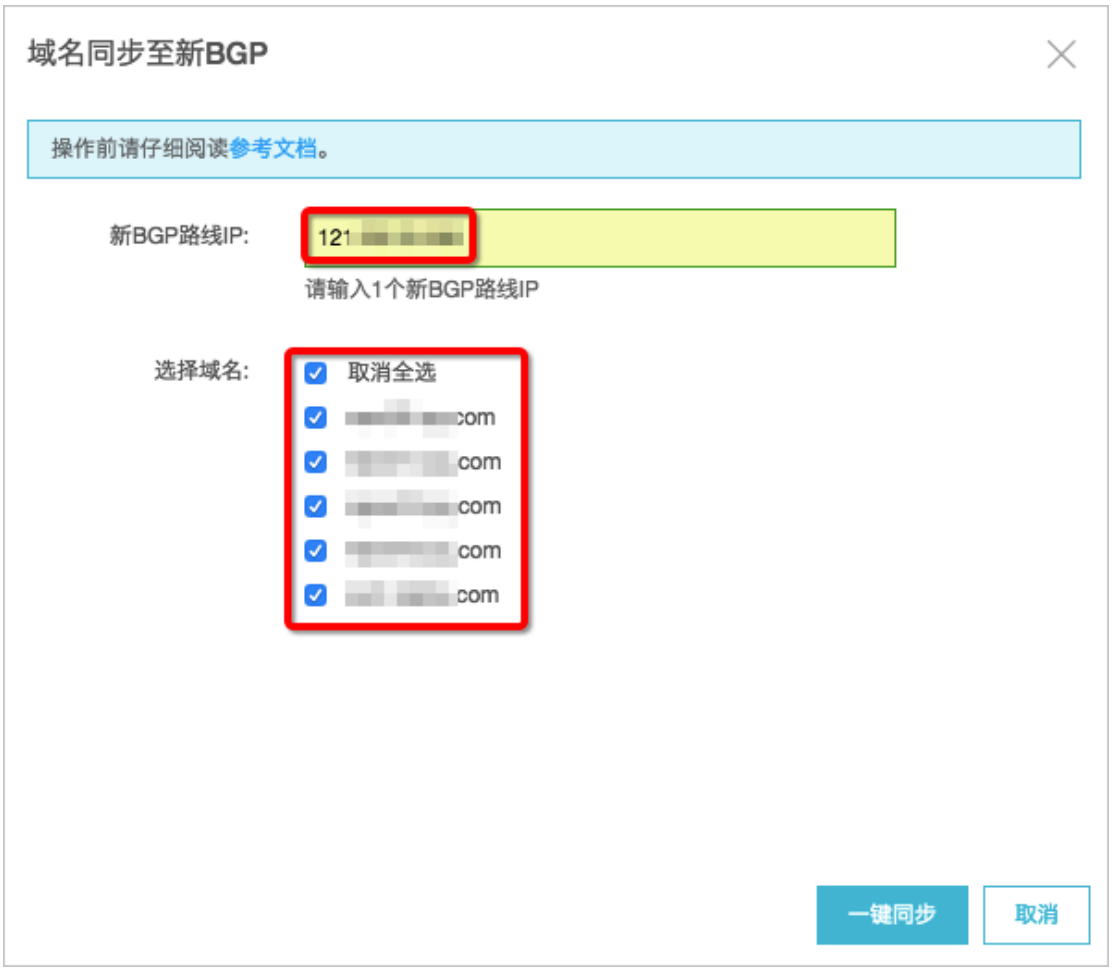
  a. 定位到接入 > 网站，单击域名同步至新BGP。

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

  说明：

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



c. 单击一键同步，并确认，将所选择的域名配置迁移至新BGP高防IP实例。您可以在新BGP高防IP管理控制台的管理 > 网站配置页面中查看已迁移的域名配置信息。

说明:

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

域名同步操作注意事项：

- 如果所需迁移的域名配置仅关联一个高防IP实例，您只需按上述步骤将所有域名配置同步至新BGP高防IP即可。
- 如果您拥有多个高防IP实例，且部分域名关联多个高防IP实例，则必须先明确所需迁移的域名及这些域名当前已关联的高防IP实例情况。如果其中存在部分高防IP实例

将继续使用且短期内不会释放，建议您先将所需迁移的域名与这些高防IP实例解除关联，再按上述步骤进行迁移。

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

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

域名配置迁移后注意事项：

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

· 非网站业务配置迁移

a. 定位到接入 > 非网站，选择所需迁移的高防IP实例和高防IP。

b. 单击导出规则/配置，选择导出规则。

c. 在新BGP高防IP管理控制台的管理 > 端口配置页面，选择实例，单击批量操作，选择添加规则。

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

> **说明:**
> 关于配置的批量导入导出的具体操作，参考业务配置批量导入导出。同时，在完成端口配置迁移后，您也可以通过该方式将原高防IP实例中非网站业务的会话保持/健康检查配置或DDoS防护策略配置迁移至新BGP高防IP。

3. 参考本地验证配置通过本地修改Host文件的方式绑定新BGP高防IP实例的IP，逐条检查网站和非网站配置是否生效。

4. 验证通过后，前往您域名对应的DNS服务商提供的域名解析管理页面，修改域名DNS解析设置，通过A记录的方式，将域名解析指向新BGP高防IP实例。

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

5. 在您确认所有业务均已迁移至新BGP高防IP实例后，如果您的原高防IP实例仍在服务期内，您可以通过工单申请退回原高防IP实例的余款。

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

其它注意事项

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

常见问题

新BGP高防IP产品有哪些优势?

关于新BGP高防IP的优势，请查看什么是新BGP高防IP。

新BGP高防IP产品的价格明细?

关于新BGP高防IP产品的产品定价，请查看新BGP高防IP计费方式。

新BGP高防IP产品的链路质量如何?

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

测试IP：203.107.32.57

业务迁移至新BGP高防IP大约需要多久?

- 网站类业务：通常由于DNS刷新等原因，需要1-3天左右完成。
- IP类业务：需要根据您的业务实际情况进行评估。

业务迁移会导致业务中断吗?

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

整个迁移过程中，阿里云都将以保障您的业务访问作为第一优先级。

迁移至新BGP高防IP还有哪些注意事项?

- 新BGP高防IP实例使用的是BGP线路的IP，天然具备故障发生时的自动切换线路能力（且相比通过DNS解析切换更快、更稳定）。因此，新BGP高防IP服务不支持通过CNAME方式接入，您需要以A记录的方式接入新BGP高防IP实例。
- 新BGP高防IP实例的回源IP段信息与原高防IP实例不同。如果您在高防IP实例后端配置了回源IP地址限制等策略，您需要手动更新回源IP段信息。

4.11 新BGP高防IP抗D包

新BGP高防IP抗D包是面向新BGP高防IP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。

新BGP高防IP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。抗D包的主要规格参数是：防护规格和可用防护次数。以300G防护规格，可用防护3次的抗D包为例，其中，

- 防护规格300G：表示该抗D包最高可抵扣保底防护带宽+300G 的攻击峰值所产生的后付费。假如攻击峰值大于保底防护值+300G，那么300G抗D包将抵扣失败；抵扣失败时，如果符合新BGP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。

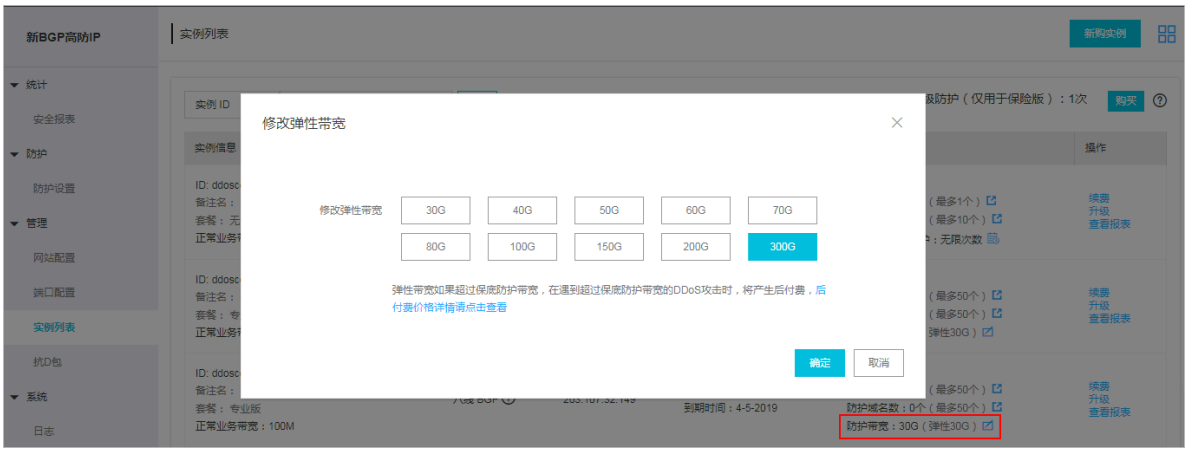
注意事项

使用新BGP高防IP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“保底防护值+抗D包规格”。

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



- **只有当攻击峰值-保底防护值=<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，使其等于保底防护值。**
- **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。**

表 4-3: 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。	无需绑定新BGP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，新BGP高防IP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：

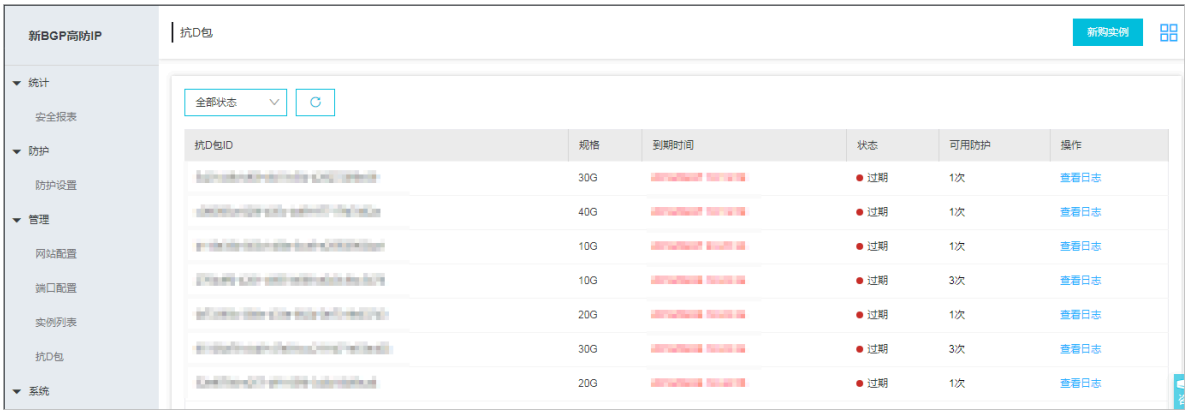
- 首次开通新BGP高防IP
- 首次连续使用新BGP高防IP 3个月以上
- 包年开通新BGP高防IP

如何使用抗D包

获得新BGP高防IP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，您可以在新BGP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。

参照以下步骤查看抗D包详情和消费记录：

1. 登录新BGP高防IP管理控制台。
2. 前往管理 > 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、耗尽和过期。
   - 可用防护：抗D包的可用防护次数。



3. 单击一个抗D包下的查看日志可以查询其操作记录。

5 API 参考

5.1 API概览

本文档汇总了BGP高防IP所有可调用的API，具体接口信息请参阅相关文档。

关于更多API资源，请访问*API Explorer*。

实例

API	描述
DescribeInstances	查询实例列表。
DescribeInstanceDetails	查询实例详情列表。
DescribeInstanceSpecs	查询实例规格列表。
DescribeInstanceStatistics	查询实例统计信息。
DescribeElasticBandwidthSpec	查询弹性带宽规格。
ModifyElasticBandWidth	修改弹性防护带宽。
ModifyInstanceRemark	修改实例备注信息。

4层规则

API	描述
CreateLayer4Rule	创建4层转发规则。
ConfigLayer4Rule	编辑4层转发规则。
DeleteLayer4Rule	删除4层转发规则。
ConfigLayer4RuleAttribute	配置4层转发规则属性（会话保持和DDoS防护策略）。
ConfigHealthCheck	配置4层/7层健康检查。
DescribeLayer4Rules	查询四层转发规则列表。
DescribeLayer4RuleAttributes	查询四层转发属性列表（会话保持和DDoS防护策略）。
DescribeHealthCheckList	查询4层/7层健康检查列表。
DescribeHealthCheckStatusList	查询健康检查状态。

7层规则

API	描述
DescribeDomains	查询7层转发规则。
CreateLayer7Rule	创建7层转发规则。
ConfigLayer7Rule	编辑7层转发规则。
DeleteLayer7Rule	删除7层转发规则。
ConfigLayer7Cert	设置证书。
ConfigLayer7BlackWhiteList	设置7层防护黑白名单。
DescribleLayer7InstanceRelations	查询7层防护实例对应关系。
DescribleCertList	查询证书列表。
EnableLayer7CC	启用7层CC防护。
DisableLayer7CC	禁用7层CC防护。
EnableLayer7CCRule	启用7层CC规则。
DisableLayer7CCRule	禁用7层CC规则。
AddLayer7CCRule	添加7层CC规则。
ConfigLayer7CCRule	编辑7层CC规则。
DescribeLayer7CCRules	查询7层CC规则。
DeleteLayer7CCRule	删除7层CC规则。
ConfigLayer7CCTemplate	设置7层CC防护模板。
DescribeDomainAccessMode	查询域名接入模式。
ConfigDomainAccessMode	设置域名接入模式。
DescribeBackSourceCidr	查询回源网段。

事件任务

API	描述
ListAsyncTask	查询异步任务列表。
CreateAsyncTask	创建异步任务。
DeleteAsyncTask	删除异步任务。

日志

API	描述
DescribeOpEntities	查询操作日志。

5.2 调用方式

BGP高防IP接口调用是向BGP高防IP的API的服务端地址发送HTTP GET请求，并按照接口说明在请求中加入相应请求参数，调用后系统会返回处理结果。请求及返回结果都使用UTF-8字符集进行编码。

请求结构

BGP高防IP的API是RPC风格，您可以通过发送HTTP GET请求调用BGP高防IP API。

其请求结构如下：

```
https://Endpoint/?Action=xx&Parameters
```

其中：

- `Endpoint`：**BGP高防IP API的服务接入地址为**`ddoscoo.cn-hangzhou.aliyuncs.com`。
- `Action`：**要执行的操作，如使用**`DescribeInstances`**，查询所有实例列表。**
- `Version`：**要使用的API版本，BGP高防IP的API版本是**`2017-12-28`。
- `Parameters`：**请求参数，每个参数之间用“&”分隔。**
- **请求参数由公共请求参数和API自定义参数组成。公共参数中包含API版本号、身份验证等信息，详情参见公共参数。**

下面是一个调用DescribeInstances接口查询所有BGP高防IP实例列表的示例：

说明：

为了便于您查看，本文档中的示例都做了格式化处理。

```
https://ddoscoo.cn-hangzhou.aliyuncs.com/?Action=DescribeInstances
&Region=cn
&InstanceId=ddoscoo-cn-XXXX1
&Format=xml
&Version=2017-12-28
&Signature=xxxx%xxxx%3D
&SignatureMethod=HMAC-SHA1
&SignatureNonce=15215528852396
&SignatureVersion=1.0
&AccessKeyId=key-test
&TimeStamp=2012-06-01T12:00:00Z
```

```
...
```

API授权

为了确保您的账号安全，建议您使用子账号的身份凭证调用API。如果您使用RAM账号调用BGP高防IP API，您需要为该RAM账号创建、附加相应的授权策略。

API签名

BGP高防IP服务会对每个API请求进行身份验证，无论使用HTTP还是HTTPS协议提交请求，都需要在请求中包含签名（Signature）信息。

BGP高防IP通过使用AccessKey ID和AccessKey Secret进行对称加密的方法来验证请求的发送者身份。AccessKey是为阿里云账号和RAM用户发布的一种身份凭证（类似于用户的登录密码），其中AccessKey ID用于标识访问者的身份，AccessKey Secret是用于加密签名字符串和服务器端验证签名字符串的密钥，必须严格保密。

RPC API需按如下格式在请求中增加签名（Signature）：

```
https://endpoint/?SignatureVersion=1.0&SignatureMethod=HMAC-SHA1&
Signature=CT9X0VtwR86fNWSnsc6v8YGOjuE%3D&SignatureNonce=3ee8c1b8-83d3-
44af-a94f-4e0ad82fd6cf
```

以DescribeInstances为例，假设AccessKey ID是 testid， AccessKey Secret是 testsecret，则签名前的请求URL如下：

```
https://ddoscoo.cn-hangzhou.aliyuncs.com/?Action=DescribeInstances
&Region=cn
&InstanceId=ddoscoo-cn-XXXX1
&TimeStamp=2016-02-23T12:46:24Z
&Format=XML
&AccessKeyId=testid
&SignatureMethod=HMAC-SHA1
&SignatureNonce=3ee8c1b8-83d3-44af-a94f-4e0ad82fd6cf
&Version=2017-12-28
&SignatureVersion=1.0
```

完成以下步骤计算签名：

1. 使用请求参数创建待签名字符串：

```
GET&%2F&AccessKeyId%3Dtestid&Action%3DDescribeDomainNames&Region
%3Dcn&InstanceId%3Dwaf_elasticity-cn-0xldbqtm005&Format%3DXML&
SignatureMethod%3DHMAC-SHA1&SignatureNonce%3D3ee8c1b8-83d3-44af-
```

```
a94f-4e0ad82fd6cf&SignatureVersion%3D1.0&TimeStamp%3D2016-02-23T12%
253A46%253A24Z&Version%3D2018-01-17
```

2. **计算待签名的HMAC的值。**

   在AccessKey Secret后添加一个“&”作为计算HMAC值的key。本示例中的key为 `testsecret&`。

```
CT9X0VtwR86fNWSnsc6v8YGOjuE=
```

3. **将签名加到请求参数中：**

```
https://ddoscoo.cn-hangzhou.aliyuncs.com/?Action=DescribeInstances
&Region=cn
&InstanceId=ddoscoo-cn-XXXX1
&TimeStamp=2016-02-23T12:46:24Z
&Format=XML
&AccessKeyId=testid
&SignatureMethod=HMAC-SHA1
&SignatureNonce=3ee8c1b8-83d3-44af-a94f-4e0ad82fd6cf
&Version=2017-12-28
&SignatureVersion=1.0
&Signature=CT9X0VtwR86fNWSnsc6v8YGOjuE%3D
```

5.3 公共参数

介绍调用新BGP高防IP API时要用到的公共参数。

公共请求参数

公共请求参数是每个接口都需要使用到的请求参数。

名称	类型	是否必需	描述
Region	String	是	BGP高防IP实例所在的地域。取值：cn-hangzhou（表示中国大陆地区）。
Format	String	否	返回消息的格式。取值： · JSON（默认） · XML
Version	String	是	API版本号，使用YYYY-MM-DD日期格式。取值：2017-12-28。
AccessKeyId	String	是	访问服务使用的密钥ID。
Signature	String	是	签名结果串。
SignatureMethod	String	是	签名方式，取值：HMAC-SHA1。

名称	类型	是否必需	描述
Timestamp	String	是	请求的时间戳，为日期格式。使用UTC时间按照ISO8601标，格式为YYYY-MM-DDThh:mm:ssZ。例如，北京时间2013年1月10日20点0分0秒，表示为2013-01-10T12:00:00Z。
SignatureVersion	String	是	签名算法版本，取值：1。
SignatureNonce	String	是	唯一随机数，用于防止网络重放攻击。在不同请求间要使用不同的随机数值。
ResourceOwnerAccount	String	否	本次API请求访问到的资源拥有者账户，即登录用户名。

示例

```
https://ddoscoo.cn-hangzhou.aliyuncs.com/?Action=DescribeInstances
&Region=cn
&InstanceId=ddoscoo-cn-XXXX1
&Timestamp=2014-05-19T10%3A33%3A56Z
&Format=xml
&AccessKeyId=testid
&SignatureMethod=Hmac-SHA1
&SignatureNonce=NwDAxvLU6tFE0DVb
&Version=2017-12-28
&SignatureVersion=1.0
&Signature=Signature
```

公共返回参数

API返回结果采用统一格式，返回2xx HTTP状态码代表调用成功；返回4xx或5xx HTTP状态码代表调用失败。调用成功返回的数据格式有XML和JSON两种，可以在发送请求时指定返回的数据格式，默认为XML格式。

每次接口调用，无论成功与否，系统都会返回一个唯一识别码 RequestId。

- XML格式

```
<?xml version="1.0" encoding="utf-8"?>
    <!--结果的根结点-->
    <接口名称+Response>
        <!--返回请求标签-->
        <RequestId>4C467B38-3910-447D-87BC-AC049166F216</RequestId>
        <!--返回结果数据-->
    </接口名称+Response>
```

- JSON格式

```
{
    "RequestId":"4C467B38-3910-447D-87BC-AC049166F216",
    /*返回结果数据*/
```

```
    }
```

5.4 实例

5.4.1 DescribeInstances

调用DescribeInstances分页查询新BGP高防实例信息列表。

调试

您可以在*OpenAPI Explorer*中直接运行该接口，免去您计算签名的困扰。运行成功后，*OpenAPI Explorer*可以自动生成*SDK*代码示例。

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	DescribeInstances	系统规定参数。取值：DescribeInstances。
PageNo	String	是	1	分页页号，即从几页开始显示。最小值是1。
PageSize	String	是	10	分页大小，即每页显示多少条结果。最大值是50。
InstanceIds	String	否	["ddoscoo-cn-XXXXX"]	通过实例Id查询实例信息，传入要查询的实例Id数组（JSON字符串）。支持精确匹配。例如，\"*ddoscoo-cn-XXXX1", "ddoscoo-cn-XXXX2"*。 **说明:** 若传入该参数，则无需传入Ip和Remark。

名称	类型	是否必选	示例值	描述
Ip	String	否	1.1.1.1	通过实例Ip查询实例信息，传入要查询的实例Ip地址。支持精确匹配查询。  说明: 若传入该参数，则无需传入InstanceIds和Remark。
Remark	String	否	testRemark	通过实例备注查询实例信息，传入要查询的实例的备注信息。支持模糊查询。  说明: 若传入该参数，则无需传入InstanceIds和Ip。

返回数据

名称	类型	示例值	描述
Instances			实例信息列表。
ExpireTime	Long	2308402384	过期时间时间戳，单位：毫秒。
GmtCreate	Long	2308402384	创建时间时间戳，单位：毫秒。
InstanceId	String	ddoscoo-cn-XXXXX	实例ID。
Remark	String	testRemark	实例备注信息。最大500字节。
Status	Integer	1	实例售卖状态。 · 1：正常 · 2：过期 · 3：释放
RequestId	String	CF33B4C3-196E-4015-AADD-5CAD00057B80	本次请求的ID。

名称	类型	示例值	描述
Total	Long	10	实例总数。

示例

请求示例

```
http(s)://ddoscoo.cn-hangzhou.aliyuncs.com/?Action=DescribeInstances
&PageNo=1
&PageSize=10
&<公共请求参数>
```

正常返回示例

`XML` **格式**

```
<DescribeInstancesResponse>
     <Instances>
          <element>
               <ExpireTime>20384032</ExpireTime>
               <GmtCreate>2308402384</GmtCreate>
               <InstanceId>0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc</
InstanceId>
               <Remark>xxx</Remark>
               <Status>1</Status>
          </element>
     </Instances>
     <RequestId>0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc</RequestId>
     <Total>1</Total>
</DescribeInstancesResponse>
```

`JSON` **格式**

```
{
 "RequestId":"0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc",
 "Instances":[
  {
   "Status":1,
   "ExpireTime":20384032,
   "InstanceId":"0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc",
   "GmtCreate":2308402384,
   "Remark":"xxx"
  }
 ],
 "Total":1
}
```

错误码

访问错误中心查看更多错误码。

5.4.2 DescribeInstanceDetails

调用DescribeInstanceDetails查询指定实例的详情信息。

调试

您可以在*OpenAPI Explorer*中直接运行该接口，免去您计算签名的困扰。运行成功后，*OpenAPI Explorer*可以自动生成*SDK*代码示例。

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	DescribeInstanceDetails	系统规定参数。取值：DescribeInstanceDetails。
InstanceIds	String	是	[{"InstanceId":"ddoscoo-cn-XXXXX","InstanceId":"ddoscoo-cn-YYYYY"}]	要查询的实例ID数组（JSON字符串）。

返回数据

名称	类型	示例值	描述
InstanceDetails			实例详情列表。
EipInfoList			与该实例绑定的EIP信息列表。
Eip	String	1.1.1.1	EIP值。
Status	String	normal	EIP状态，取值： · normal：正常 · cleaning：清洗中 · blackhole：黑洞中
InstanceId	String	ddoscoo-cn-XXXXX	实例ID。
Line	String	coop-line-001	实例线路。例如，coop-line-001。
RequestId	String	CF33B4C3-196E-4015-AADD-5CAD00057B80	本次请求的ID。

示例

请求示例

```
http(s)://[Endpoint]/?Action=DescribeInstanceDetails
&InstanceIds=[{"InstanceId":"ddoscoo-cn-XXXXX","InstanceId":"ddoscoo-
cn-YYYYY"}]
&<公共请求参数>
```

正常返回示例

`XML` **格式**

```
<DescribeInstanceDetailsResponse>
     <InstanceDetails>
          <element>
               <EipInfoList>
                    <element>
                         <Eip>1.1.1.1</Eip>
                         <Status>normal</Status>
                    </element>
               </EipInfoList>
               <InstanceId>0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc</
InstanceId>
               <Line>coop-line-001</Line>
          </element>
     </InstanceDetails>
     <RequestId>0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc</RequestId>
</DescribeInstanceDetailsResponse>
```

`JSON` **格式**

```
{
 "InstanceDetails":[
  {
   "InstanceId":"0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc",
   "Line":"coop-line-001",
   "EipInfoList":[
    {
     "Status":"normal",
     "Eip":"1.1.1.1"
    }
   ]
  }
 ],
 "RequestId":"0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc"
}
```

错误码

访问错误中心查看更多错误码。

5.4.3 DescribeInstanceSpecs

调用DescribeInstanceSpecs查询指定实例的规格。

调试

您可以在*OpenAPI Explorer*中直接运行该接口，免去您计算签名的困扰。运行成功后，*OpenAPI Explorer*可以自动生成*SDK*代码示例。

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	DescribeInstanceSpecs	系统规定参数。取值：DescribeInstanceSpecs。
InstanceIds	String	是	["ddoscoo-cn-XXXXX"]	要查询的实例ID数组（JSON字符串）。

返回数据

名称	类型	示例值	描述
InstanceSpecs			实例规格列表。
BandwidthMbps	Integer	20000	业务带宽值。
BaseBandwidth	Integer	20	基础带宽值。
DefenseCount	Integer	10	防护次数。
DomainLimit	Integer	50	最大域名个数。
ElasticBandwidth	Integer	20	弹性带宽值。
FunctionVersion	String	default	功能版本，取值： · default：标准版 · enhance：增强版
InstanceId	String	ddoscoo-cn-XXXXX	实例ID。
PortLimit	Integer	50	最大四层转发次数。

名称	类型	示例值	描述
QpsLimit	Integer	1000	QPS限制。
SiteLimit	Integer	10	站点防护数限制。
RequestId	String	CF33B4C3-196E-4015-AADD-5CAD00057B80	本次请求的ID。

示例

请求示例

```
http(s)://[Endpoint]/?Action=DescribeInstanceSpecs
&InstanceIds=["ddoscoo-cn-XXXXX"]
&<公共请求参数>
```

正常返回示例

`XML` **格式**

```
<DescribeInstanceSpecsResponse>
     <InstanceSpecs>
          <element>
               <BandwidthMbps>100</BandwidthMbps>
               <BaseBandwidth>20</BaseBandwidth>
               <DefenseCount>10</DefenseCount>
               <DomainLimit>20</DomainLimit>
               <ElasticBandwidth>10</ElasticBandwidth>
               <FunctionVersion>default</FunctionVersion>
               <InstanceId>0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc</
InstanceId>
               <PortLimit>10</PortLimit>
               <SiteLimit>10</SiteLimit>
               <QpsLimit>1000</QpsLimit>
          </element>
     </InstanceSpecs>
     <RequestId>0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc</RequestId>
</DescribeInstanceSpecsResponse>
```

`JSON` **格式**

```
{
 "InstanceSpecs":[
  {
   "QpsLimit":1000,
   "DomainLimit":20,
   "FunctionVersion":"default",
   "SiteLimit":10,
   "BandwidthMbps":100,
   "PortLimit":10,
   "DefenseCount":10,
   "InstanceId":"0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc",
   "ElasticBandwidth":10,
```

```
    "BaseBandwidth":20
  }
 ],
 "RequestId":"0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc"
}
```

错误码

访问错误中心查看更多错误码。

5.4.4 DescribeInstanceStatistics

调用DescribeInstanceStatistics查询指定实例的统计信息。

调试

您可以在*OpenAPI Explorer*中直接运行该接口，免去您计算签名的困扰。运行成功后，*OpenAPI Explorer*可以自动生成*SDK*代码示例。

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	DescribeInstanceStatistics	系统规定参数。取值：DescribeInstanceStatistics。
InstanceIds	String	是	[{"InstanceId":"ddoscoo-cn-XXXXX","InstanceId":"ddoscoo-cn-YYYYY"}]	要查询的实例ID数组（JSON字符串）。

返回数据

名称	类型	示例值	描述
InstanceStatistics			实例的统计信息列表。
DefenseCountUsage	Integer	1	已使用防护次数。
DomainUsage	Integer	10	已使用域名的数量。
InstanceId	String	ddoscoo-cn-XXXXX	实例ID。
PortUsage	Integer	20	已使用四层规则的数量。

名称	类型	示例值	描述
SiteUsage	Integer	1	已添加站点的数量。
RequestId	String	CF33B4C3-196E-4015-AADD-5CAD00057B80	本次请求的ID。

示例

请求示例

```
http(s)://[Endpoint]/?Action=DescribeInstanceStatistics
&InstanceIds=[{"InstanceId":"ddoscoo-cn-XXXXX","InstanceId":"ddoscoo-
cn-YYYYY"}]
&<公共请求参数>
```

正常返回示例

`XML` **格式**

```
<DescribeInstanceStatisticsResponse>
     <InstanceStatistics>
          <element>
               <DomainUsage>10</DomainUsage>
               <InstanceId>0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc</
InstanceId>
               <PortUsage>20</PortUsage>
          </element>
     </InstanceStatistics>
     <RequestId>0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc</RequestId>
</DescribeInstanceStatisticsResponse>
```

`JSON` **格式**

```
{
 "RequestId":"0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc",
 "InstanceStatistics":[
  {
   "DomainUsage":10,
   "PortUsage":20,
   "InstanceId":"0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc"
  }
 ]
}
```

错误码

访问错误中心查看更多错误码。

5.4.5 DescribeElasticBandwidthSpec

调用DescribeElasticBandwidthSpec查询指定实例的弹性带宽规格。

调试

您可以在*OpenAPI Explorer*中直接运行该接口，免去您计算签名的困扰。运行成功后，*OpenAPI Explorer*可以自动生成*SDK*代码示例。

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	DescribeElasticBandwidthSpec	系统规定参数。取值：DescribeElasticBandwidthSpec。
InstanceId	String	是	ddoscoo-cn-XXXXX	要查询的实例ID。单次请求只支持查询1个实例。

返回数据

名称	类型	示例值	描述
ElasticBandwidthSpec		[5, 10, 20, 30]	弹性带宽规格。
RequestId	String	CF33B4C3-196E-4015-AADD-5CAD00057B80	本次请求的ID。

示例

请求示例

```
http(s)://[Endpoint]/?Action=DescribeElasticBandwidthSpec
&InstanceId=ddoscoo-cn-XXXXX
&<公共请求参数>
```

正常返回示例

`XML` **格式**

```
<DescribeElasticBandwidthSpecResponse>
     <ElasticBandwidthSpec>
          <element>5</element>
          <element>10</element>
          <element>20</element>
          <element>30</element>
     </ElasticBandwidthSpec>
     <RequestId>0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc</RequestId>
```

```
</DescribeElasticBandwidthSpecResponse>
```

JSON 格式

```
{
 "RequestId":"0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc",
 "ElasticBandwidthSpec":[
  5,
  10,
  20,
  30
 ]
}
```

错误码

访问错误中心查看更多错误码。

5.4.6 ModifyElasticBandWidth

调用ModifyElasticBandWidth修改指定实例的弹性防护带宽。

调试

您可以在*OpenAPI Explorer*中直接运行该接口，免去您计算签名的困扰。运行成功后，*OpenAPI Explorer*可以自动生成*SDK*代码示例。

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	ModifyElasticBandWidth	系统规定参数。取值：ModifyElasticBandWidth。
ElasticBandwidth	Integer	是	30	新的弹性带宽值。
InstanceId	String	是	ddoscoo-cn-XXXXX	要操作的实例ID。单次请求只支持修改1个实例的弹性防护带宽，且目标实例必须是正常状态。

返回数据

名称	类型	示例值	描述
RequestId	String	CF33B4C3-196E-4015-AADD-5CAD00057B80	本次请求的ID。

示例

请求示例

```
http(s)://[Endpoint]/?Action=ModifyElasticBandWidth
&ElasticBandwidth=30
&InstanceId=ddoscoo-cn-XXXXX
&<公共请求参数>
```

正常返回示例

`XML` **格式**

```
<ModifyElasticBandWidthResponse>
     <RequestId>0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc</RequestId>
</ModifyElasticBandWidthResponse>
```

`JSON` **格式**

```
{
 "RequestId":"0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc"
}
```

错误码

访问错误中心查看更多错误码。

5.4.7 ModifyInstanceRemark

调用ModifyInstanceRemark修改指定实例的备注信息。

请求参数

名称	类型	是否必需	描述
InstanceId	String	是	要操作的实例ID。单次请求只支持修改1个实例的备注信息。
Remark	String	是	新的备注信息。

返回参数

名称	类型	描述
RequestId	String	本次请求的ID。

示例

请求示例

```
{
  "InstanceId": "0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc",
```

```
  "Remark": "huadong2"
}
```

返回示例

```
{
  "RequestId": "0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc"
}
```

5.5 四层规则

5.5.1 CreateLayer4Rule

调用CreateLayer4Rule创建4层转发规则。

调试

您可以在*OpenAPI Explorer*中直接运行该接口，免去您计算签名的困扰。运行成功后，*OpenAPI Explorer*可以自动生成*SDK*代码示例。

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	CreateLayer4Rule	系统规定参数。取值：CreateLayer4Rule。
Listeners	String	是	[{"InstanceId":"xxxxxx-xxxxxx-xxxxxx-xxxxxxx","Protocol":"tcp","FrontendPort":80,"BackendPort":5,"RealServers":"1.1.1.1","2.2.2.2"}]	传入要操作的Listeners的JSON数组串，每个Listener的具体结构描述如下： · InstanceId，String类型，必选，实例ID。 · Protocol，String类型，必选，协议类型。 · FrontendPort，Integer类型，必选，前端使用的端口，取值范围：0-65535。 · BackendPort，Integer类型，必选，后端使用的端口，取值范围：0-65535。 · RealServers，Json数组类型，必选，源站IP地址。

返回数据

名称	类型	示例值	描述
RequestId	String	CF33B4C3-196E-4015-AADD-5CAD00057B80	本次请求的ID。

示例

请求示例

```
http(s)://[Endpoint]/?Action=CreateLayer4Rule
&Listeners=[{"InstanceId":"xxxxxx-xxxxxx-xxxxxx-xxxxxxx","Protocol":"
tcp","FrontendPort":80,"BackendPort":5,"RealServers":"1.1.1.1","2.2.2.
2"}]
&<公共请求参数>
```

正常返回示例

`XML` **格式**

```
<CreateLayer4RuleResponse>
     <RequestId>0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc</RequestId>
</CreateLayer4RuleResponse>
```

`JSON` **格式**

```
{
 "RequestId":"0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc"
}
```

错误码

访问错误中心查看更多错误码。

5.5.2 ConfigLayer4Rule

调用ConfigLayer4Rule编辑4层转发规则。

调试

您可以在*OpenAPI Explorer*中直接运行该接口，免去您计算签名的困扰。运行成功后，*OpenAPI Explorer*可以自动生成*SDK*代码示例。

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	ConfigLayer4Rule	系统规定参数。取值：ConfigLayer4Rule。
Listeners	String	是	[{"InstanceId":"xxxxxx-xxxxxx-xxxxxx-xxxxxxx","Protocol":"tcp","FrontendPort":80,"BackendPort":5,"RealServers":"1.1.1.1","2.2.2.2"}]	传入要操作的Listeners的JSON数组串，每个Listener的具体结构描述如下。 · InstanceId，String类型，必选，实例ID。 · Protocol，String类型，必选，协议类型。 · FrontendPort，Integer类型，必选，前端使用的端口，取值范围：0-65535。 · BackendPort，Integer类型，必选，后端使用的端口，取值范围：0-65535。 · RealServers，Json数组类型，必选，源站IP地址。

返回数据

名称	类型	示例值	描述
RequestId	String	0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc	本次请求的ID。

示例

请求示例

```
http(s)://[Endpoint]/?Action=ConfigLayer4Rule
&Listeners=[{"InstanceId":"xxxxxx-xxxxxx-xxxxxx-xxxxxxx","Protocol":"
tcp","FrontendPort":80,"BackendPort":5,"RealServers":"1.1.1.1","2.2.2.
2"}]
&<公共请求参数>
```

正常返回示例

`XML` **格式**

```
<ConfigLayer4RuleResponse>
```

```
    <RequestId>0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc</RequestId>
</ConfigLayer4RuleResponse>
```

JSON 格式

```
{
 "RequestId":"0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc"
}
```

错误码

访问错误中心查看更多错误码。

5.5.3 DeleteLayer4Rule

调用DeleteLayer4Rule删除4层转发规则。

调试

您可以在*OpenAPI Explorer*中直接运行该接口，免去您计算签名的困扰。运行成功后，*OpenAPI Explorer*可以自动生成*SDK*代码示例。

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	DeleteLayer4Rule	系统规定参数。取值：DeleteLayer4Rule。
Listeners	String	是	{"InstanceId":"0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc","Protocol":"tcp","FrontendPort":80}	传入要操作的Listeners的JSON数组串，每个Listener的具体结构描述如下： 说明: 目前不支持批量删除，每次只允许删除一个对象。 · InstanceId，String类型，必选，实例ID。 · Protocol，String类型，必选，协议类型。 · FrontendPort，Integer类型，必选，前端使用的端口，取值范围：0-65535。

返回数据

名称	类型	示例值	描述
RequestId	String	CF33B4C3-196E-4015-AADD-5CAD00057B80	本次请求的ID。

示例

请求示例

```
http(s)://[Endpoint]/?Action=DeleteLayer4Rule
&Listeners={"InstanceId":"0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc","
Protocol":"tcp","FrontendPort":80}
&<公共请求参数>
```

正常返回示例

`XML` **格式**

```
<DeleteLayer4RuleResponse>
      <RequestId>0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc</RequestId>
</DeleteLayer4RuleResponse>
```

`JSON` **格式**

```
{
 "RequestId":"0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc"
}
```

错误码

访问**错误中心**查看更多错误码。

5.5.4 ConfigLayer4RuleAttribute

调用ConfigLayer4RuleAttribute配置4层转发规则属性，包括会话保持和DDoS防护策略。

调试

您可以在*OpenAPI Explorer*中直接运行该接口，免去您计算签名的困扰。运行成功后，*OpenAPI Explorer*可以自动生成*SDK*代码示例。

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	ConfigLayer4RuleAttribute	系统规定参数。取值：ConfigLayer4RuleAttribute。

名称	类型	是否必选	示例值	描述
Config	String	是	{"Slimit":{"CpsEnable":1,"MaxconnEnable":1,"Cps":1,"Maxconn":1},"Sla":{"CpsEnable":1,"MaxconnEnable":1,"Cps":100,"Maxconn":1000},"PayloadLen":{"Min":0,"Max":6000}}	配置信息，传入TcpConfig或UdpConfig对象JSON串。 TcpConfig的具体结构描述见如下： · PersistenceTimeout，Integer类型，必选，会话保持的超时时间，单位为秒。默认为0，表示关闭。 · Synproxy，String类型，必选，DDoS防护策略的虚假源，取值：off、on。 · NodataConn，String类型，必选，DDoS防护策略的空连接，取值：off、on。 · Sla，Struct类型，必选，目的限制配置。具体结构描述见Sla。 · Slimit，Struct类型，必选，源限制配置。具体结构描述见Slimit。 · PayloadLen，Struct类型，必选，包过滤配置。具体结构描述见PayloadLen。 UdpConfig的具体结构描述如下： · PersistenceTimeout，Integer类型，必选，会话保持的超时时间，单位为秒。默认为0，表示关闭。 · Synproxy，String类型，必选，DDoS防护策略的虚假源，取值：off、on。 · NodataConn，String类型，必选，DDoS防护策略的空连接，取值：off、on。 · Sla，Struct类型，必选，目的限制配置。具体结构描述见Sla。 · Slimit，Struct类型，必选，源限制配置。具体结构描述见Slimit。 · PayloadLen，Struct类型，必选，包过滤配置。具体结构描述见PayloadLen。 Sla的具体结构描述如下：

名称	类型	是否必选	示例值	描述
ForwardProtocol	String	是	TCP	转发协议，取值：TCP、UDP。
FrontendPort	Integer	是	233	前端端口。
InstanceId	String	是	ddoscoo-cn-XXXXX	要操作的实例ID。

返回数据

名称	类型	示例值	描述
RequestId	String	CF33B4C3-196E-4015-AADD-5CAD00057B80	本次请求的ID。

示例

请求示例

```
http(s)://[Endpoint]/?Action=ConfigLayer4RuleAttribute
&Config={"Slimit":{"CpsEnable":1,"MaxconnEnable":1,"Cps":1,"Maxconn":
1},"Sla":{"CpsEnable":1,"MaxconnEnable":1,"Cps":100,"Maxconn":1000},"
PayloadLen":{"Min":0,"Max":6000}}
&ForwardProtocol=TCP
&FrontendPort=233
&InstanceId=ddoscoo-cn-XXXXX
&<公共请求参数>
```

正常返回示例

`XML` **格式**

```
<ConfigLayer4RuleAttributeResponse>
     <RequestId>0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc</RequestId>
</ConfigLayer4RuleAttributeResponse>
```

`JSON` **格式**

```
{
 "RequestId":"0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc"
}
```

错误码

访问错误中心查看更多错误码。

5.5.5 ConfigHealthCheck

调用ConfigHealthCheck配置四层或七层健康检查。

调试

您可以在*OpenAPI Explorer*中直接运行该接口，免去您计算签名的困扰。运行成功后，*OpenAPI Explorer*可以自动生成*SDK*代码示例。

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	ConfigHealthCheck	系统规定参数。取值：ConfigHealthCheck。
ForwardProtocol	String	是	tcp	转发协议，取值： · TCP（四层） · UDP（四层） · HTTP（七层）
FrontendPort	Integer	是	233	前端端口。

名称	类型	是否必选	示例值	描述
HealthCheck	String	是	{"Type":"tcp","Timeout":10,"Port":80,"Interval":10,"Up":10,"Down":40}"}	传入HealthCheck对象JSON串，具体结构描述如下： · Type，String类型，必选，协议类型。取值：TCP（四层）、HTTP（七层）。 · Domain，String类型，可选，健康检查/七层健康检查/域名。 · Uri，String类型，可选，健康检查/七层健康检查/检查路径。 · Timeout，Integer类型，可选，健康检查/四层健康检查/响应超时时间。 · Port，Integer类型，可选，健康检查/四层健康检查/检查端口。 · Interval，Integer类型，可选，健康检查/四层健康检查/检查间隔。 · Up，Integer类型，可选，健康检查/四层健康检查/健康阈值。 · Down，Integer类型，可选，健康检查/四层健康检查/不健康阈值。
InstanceId	String	是	ddoscoo-cn-XXXXXX	要操作的实例ID。

返回数据

名称	类型	示例值	描述
RequestId	String	CF33B4C3-196E-4015-AADD-5CAD00057B80	本次请求的ID。

示例

请求示例

```
http(s)://[Endpoint]/?Action=ConfigHealthCheck
&ForwardProtocol=tcp
&FrontendPort=233
```

```
&HealthCheck={"Type":"tcp","Timeout":10,"Port":80,"Interval":10,"Up":
10,"Down":40}"}
&InstanceId=ddoscoo-cn-XXXXXX
&<公共请求参数>
```

正常返回示例

`XML` **格式**

```
<ConfigHealthCheckResponse>
     <RequestId>0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc</RequestId>
</ConfigHealthCheckResponse>
```

`JSON` **格式**

```
{
 "RequestId":"0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc"
}
```

错误码

访问错误中心查看更多错误码。

5.5.6 DescribeLayer4Rules

调用DescribeLayer4Rules查询指定实例的四层转发规则。

调试

您可以在*OpenAPI Explorer*中直接运行该接口，免去您计算签名的困扰。运行成功后，*OpenAPI Explorer*可以自动生成*SDK*代码示例。

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	DescribeLayer4Rules	系统规定参数。取值：DescribeLayer4Rules。
InstanceId	String	是	ddoscoo-cn-XXXXX	要查询的实例ID。
Offset	Integer	是	0	开始索引位置，即从第几个结果开始返回。 说明: 如果不传入该参数，则从第0个结果开始返回。

名称	类型	是否必选	示例值	描述
PageSize	String	是	50	分页大小，即每页显示多少个结果。最大值50。
ForwardProtocol	String	否	tcp	转发协议，取值：TCP。
FrontendPort	Integer	否	233	前端端口。

返回数据

名称	类型	示例值	描述
Listeners			Listeners数组。
BackendPort	Integer	233	后端使用的端口，范围：0-65535。
FrontendPort	Integer	233	前端使用的端口，范围：0-65535。
InstanceId	String	ddoscoo-cn-XXXXX	实例ID。
IsAutoCreate	Boolean	false	是否自动创建。如果是，则不允许删除和修改。
Protocol	String	tcp	协议类型。
RealServers		["1.1.1.1"]	源站IP地址。
RequestId	String	CF33B4C3-196E-4015-AADD-5CAD00057B80	本次请求的ID。
Total	Long	10	结果总数。

示例

请求示例

```
http(s)://[Endpoint]/?Action=DescribeLayer4Rules
&InstanceId=ddoscoo-cn-XXXXX
&Offset=0
&PageSize=50
```

```
&<公共请求参数>
```

正常返回示例

`XML` **格式**

```
<DescribeLayer4RulesResponse>
     <Listeners>
          <element>
               <BackendPort>80</BackendPort>
               <FrontendPort>80</FrontendPort>
               <InstanceId>0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc</
InstanceId>
               <IsAutoCreate>true</IsAutoCreate>
               <Protocol>tcp</Protocol>
               <RealServers>
                    <element>1.1.1.1</element>
                    <element>2.2.2.2</element>
               </RealServers>
          </element>
     </Listeners>
     <RequestId>0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc</RequestId>
     <Total>1</Total>
</DescribeLayer4RulesResponse>
```

`JSON` **格式**

```
{
 "Listeners":[
  {
   "RealServers":[
    "1.1.1.1",
    "2.2.2.2"
   ],
   "BackendPort":80,
   "FrontendPort":80,
   "InstanceId":"0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc",
   "IsAutoCreate":true,
   "Protocol":"tcp"
  }
 ],
 "RequestId":"0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc",
 "Total":1
}
```

错误码

访问错误中心查看更多错误码。

5.5.7 DescribeLayer4RuleAttributes

调用DescribeLayer4RuleAttributes查询四层转发属性，包括会话保持和DDoS防护策略。

调试

您可以在*OpenAPI Explorer*中直接运行该接口，免去您计算签名的困扰。运行成功后，*OpenAPI Explorer*可以自动生成*SDK*代码示例。

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	DescribeLayer4RuleAttributes	系统规定参数。取值：DescribeLayer4RuleAttributes。
Listeners	String	是	[{"InstanceId":"ddoscoo-cn-XXXXX","Protocol":"tcp","FrontendPort":80}]	传入要查询的Listener数组JSON串，每个Listener的具体结构描述如下： · InstanceId，String类型，必选，实例ID。 · Protocol，String类型，必选，协议类型。 · FrontendPort，Integer类型，必选，前端使用的端口，取值范围：0-65535。 · BackendPort，Integer类型，可选，后端使用的端口，取值范围：0-65535。 · RealServers，Json数组类型，可选，源站IP地址。 · IsAutoCreate，Boolean类型，可选，是否自动创建。如果是，则不允许删除和修改。

返回数据

名称	类型	示例值	描述
Listeners			Listener数组JSON串。
Config			TCP配置。
NodataConn	String	on	DDoS防护策略的空连接，取值：off、on。
PayloadLen			包过滤配置。
Max	Integer	2	DDoS防护策略/包长度过滤，包长度的最大值。

名称	类型	示例值	描述
Min	Integer	1	DDoS防护策略/包长度过滤，包长度的最小值。
PersistenceTimeout	Integer	0	会话保持的超时时间，单位为秒。默认为0，表示关闭。
Sla			目的限制配置。
Cps	Integer	100	DDoS防护策略/源新建连接限速，取值范围：100~100,000。
CpsEnable	Integer	0	是否启用Cps，取值： · 0：禁用cps · 1：启用cps（默认）
Maxconn	Integer	1000	DDoS防护策略/源并发连接限速，取值范围：1,000~1,000,000。
MaxconnEnable	Integer	0	是否启用Maxconnection，取值： · 0：禁用maxconn · 1：启用maxconn（默认）
Slimit			源限制配置。
Cps	Integer	100	DDoS防护策略/源新建连接限速，取值范围：100~100,000。
CpsEnable	Integer	0	是否启用Cps，取值： · 0：禁用cps · 1：启用cps（默认）
CpsMode	Integer	2	源新建连接限速，取值： · 1：手动 · 2：自动
Maxconn	Integer	1000	DDoS防护策略/源并发连接限速，取值范围：1,000~1,000,000。

名称	类型	示例值	描述
MaxconnEnable	Integer	0	是否启用Maxconnection，取值： · 0：禁用maxconn · 1：启用maxconn（默认）
Synproxy	String	on	DDoS防护策略的虚假源，取值：off、on。
FrontendPort	Integer	233	前端使用的端口，范围：0-65535。
InstanceId	String	ddoscoo-cn-XXXXX	实例ID。
Protocol	String	tcp	协议类型。
RequestId	String	CF33B4C3-196E-4015-AADD-5CAD00057B80	本次请求的ID。

示例

请求示例

```
http(s)://[Endpoint]/?Action=DescribeLayer4RuleAttributes
&Listeners=[{"InstanceId":"ddoscoo-cn-XXXXX","Protocol":"tcp","
FrontendPort":80}]
&<公共请求参数>
```

正常返回示例

`XML` **格式**

```
<DescribeLayer4RuleAttributesResponse>
     <Listeners>
          <element>
               <Config>
                    <NodataConn>on</NodataConn>
                    <PayloadLen>
                         <Max>2</Max>
                         <Min>1</Min>
                    </PayloadLen>
                    <PersistenceTimeout>80</PersistenceTimeout>
                    <Sla>
                         <Cps>10</Cps>
                         <CpsEnable>1</CpsEnable>
                         <Maxconn>10</Maxconn>
                         <MaxconnEnable>1</MaxconnEnable>
                    </Sla>
                    <Slimit>
                         <Cps>10</Cps>
```

```
                        <CpsEnable>1</CpsEnable>
                        <Maxconn>10</Maxconn>
                        <MaxconnEnable>1</MaxconnEnable>
                    </Slimit>
                    <Synproxy>off</Synproxy>
                </Config>
                <FrontendPort>80</FrontendPort>
                <InstanceId>0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc</
InstanceId>
                <Protocol>tcp</Protocol>
            </element>
        </Listeners>
        <RequestId>0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc</RequestId>
</DescribeLayer4RuleAttributesResponse>
```

JSON 格式

```
{
 "Listeners":[
  {
   "Config":{
    "Synproxy":"off",
    "NodataConn":"on",
    "PayloadLen":{
     "Max":2,
     "Min":1
    },
    "Sla":{
     "MaxconnEnable":1,
     "Maxconn":10,
     "Cps":10,
     "CpsEnable":1
    },
    "Slimit":{
     "MaxconnEnable":1,
     "Maxconn":10,
     "Cps":10,
     "CpsEnable":1
    },
    "PersistenceTimeout":80
   },
   "FrontendPort":80,
   "InstanceId":"0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc",
   "Protocol":"tcp"
  }
 ],
 "RequestId":"0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc"
}
```

错误码

访问错误中心查看更多错误码。

5.5.8 DescribeHealthCheckList

调用DescribeHealthCheckList查询4层/7层健康检查列表。

请求参数

名称	类型	是否必需	描述
Listeners	String	是	要查询的Listeners数组JSON串，每个Listener的具体结构描述见*Listener*。

表 5-1: Listener

名称	类型	是否必需	描述
InstanceId	String	是	实例ID。
Protocol	String	是	协议类型。
FrontendPort	Integer	是	前端使用的端口，范围：0-65535。
BackendPort	Integer	否	后端使用的端口，范围：0-65535。
RealServers	Json数组	否	源站IP地址。
IsAutoCreate	Boolean	否	是否自动创建。如果是，则不允许删除和修改。

返回参数

名称	类型	描述
Total	Integer	结果总数。
HealthCheck	HealthCheck	健康检查信息。具体结构描述见*HealthCheck*。
RequestId	String	请求ID。

表 5-2: HealthCheck

名称	类型	描述
Type	String	协议类型，取值： • TCP（四层） • HTTP（七层）
Domain	String	健康检查/七层健康检查/域名。
Uri	String	健康检查/七层健康检查/检查路径。

名称	类型	描述
Timeout	Integer	健康检查/四层健康检查/响应超时时间。
Port	Integer	健康检查/四层健康检查/检查端口。
Interval	Integer	健康检查/四层健康检查/检查间隔。
Up	Integer	健康检查/四层健康检查/健康阈值。
Down	Integer	健康检查/四层健康检查/不健康阈值。

示例

请求示例

```
{
  "Listeners": "[{\"InstanceId\":\"0bcf28g5-d57c-11e7-9bs0-d89d6717dx
bc\",\"Protocol\":\"tcp\",\"FrontendPort\":80}]"
}
```

返回示例

```
{
  "Total": 1,
  "HealthCheck": [
    {
      "InstanceId": "0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc",
      "Protocol": "tcp",
      "FrontendPort": 80,
      "HealthCheck": {
        "Type": "tcp",
        "Timeout": 10,
        "Port": 80,
        "Interval": 10,
        "Up": 10,
        "Down": 20
      }
    }
  ],
  "RequestId": "0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc"
}
```

5.5.9 DescribeHealthCheckStatusList

调用DescribeHealthCheckStatusList查询健康检查状态。

查询健康检查状态列表

调试

您可以在*OpenAPI Explorer*中直接运行该接口，免去您计算签名的困扰。运行成功后，*OpenAPI Explorer*可以自动生成*SDK*代码示例。

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	DescribeHealthCheckStatusList	系统规定参数。取值：DescribeHealthCheckStatusList。
Listeners	String	是	[{"InstanceId":"ddoscoo-cn-XXXXX","Protocol":"tcp","FrontendPort":80}]	要查询的转发规则Listeners数组（JSON字符串），每个Listener的具体结构描述如下： · InstanceId，String类型，必选，实例ID。 · Protocol，String类型，必选，协议类型。 · FrontendPort，Integer类型，必选，前端使用的端口，取值范围：0-65535。 · BackendPort，Integer类型，可选，后端使用的端口，取值范围：0-65535。 · RealServers，Json数组类型，可选，源站IP地址。 · IsAutoCreate，Boolean类型，可选，是否自动创建。如果是，则不允许删除和修改。

返回数据

名称	类型	示例值	描述
HealthCheckStatusList			健康检查状态列表。
FrontendPort	Integer	233	前端端口。
InstanceId	String	ddoscoo-cn-XXXXX	实例Id。
Protocol	String	tcp	协议类型。
RealServerStatusList			源站状态JSON数组。
Address	String	1.1.1.1	源站IP。

名称	类型	示例值	描述
Status	String	normal	状态，取值：normal、abnormal。
Status	String	normal	状态，取值：normal、abnormal。
RequestId	String	CF33B4C3-196E-4015-AADD-5CAD00057B80	本次请求的ID。

示例

请求示例

```
http(s)://[Endpoint]/?Action=DescribeHealthCheckStatusList
&Listeners=[{"InstanceId":"ddoscoo-cn-XXXXX","Protocol":"tcp","
FrontendPort":80}]
&<公共请求参数>
```

正常返回示例

`XML` **格式**

```
<DescribeHealthCheckStatusListResponse>
     <HealthCheckStatusList>
          <element>
               <FrontendPort>80</FrontendPort>
               <InstanceId>0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc</
InstanceId>
               <Protocol>tcp</Protocol>
               <RealServerStatusList>
                    <Address>1.1.1.1</Address>
                    <Status>normal</Status>
               </RealServerStatusList>
               <Status>normal</Status>
          </element>
     </HealthCheckStatusList>
     <RequestId>0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc</RequestId>
</DescribeHealthCheckStatusListResponse>
```

`JSON` **格式**

```
{
 "RequestId":"0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc",
 "HealthCheckStatusList":[
  {
   "Status":"normal",
   "FrontendPort":80,
   "InstanceId":"0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc",
   "RealServerStatusList":{
    "Status":"normal",
    "Address":"1.1.1.1"
   },
   "Protocol":"tcp"
  }
```

```
  ]
}
```

错误码

访问错误中心查看更多错误码。

5.6 七层规则

5.6.1 DescribeDomains

调用DescribeDomains查询7层转发规则。

调试

您可以在*OpenAPI Explorer*中直接运行该接口，免去您计算签名的困扰。运行成功后，*OpenAPI Explorer*可以自动生成*SDK*代码示例。

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	DescribeDomains	系统规定参数。取值：DescribeDomains。
Offset	Integer	是	0	开始索引位置，即从第几条结果开始显示。默认从0开始。
PageSize	String	是	10	分页大小，即每页显示多少条记录。最大值10。
Domain	String	否	www.aliyun.com	要查询的域名。
QueryDomainPattern	String	否	fuzzy	查询匹配模式。取值： · fuzzy：模糊查询（默认） · exact：精确查询

返回数据

名称	类型	示例值	描述
RequestId	String	CF33B4C3-196E-4015-AADD-5CAD00057B80	本次请求的ID。

名称	类型	示例值	描述
Total	Long	10	域名总数。
Domains			域名列表。
BlackList		["1.1.1.1/1","1.1.1.2/2"]	黑名单IP列表。
CcEnabled	Boolean	true	是否启用CC防护。
CcRuleEnabled	Boolean	true	是否启用CC规则。
CcTemplate	String	normal	CC防护模板。
CertName	String	testCertName	证书名称。
Domain	String	www.aliyun.com	域名。
ProxyTypeList			协议类型列表。
ProxyPorts		111	协议端口。
ProxyType	String	http	协议类型。取值： · http · https · websocket · websockets
RealServers			源站列表。
RealServer	String	1.1.1.1	源站地址。
RsType	Integer	0	源站类型。取值： · 0：IP · 1：域名
WhiteList		["1.1.1.1/1","1.1.1.2/2"]	白名单IP列表。

示例

请求示例

```
http(s)://[Endpoint]/?Action=DescribeDomains
&Offset=0
&PageSize=10
&<公共请求参数>
```

正常返回示例

`XML` **格式**

```
<DescribeDomainsResponse>
     <Domains>
          <element>
               <BlackList>
                    <element>1.1.1.1/1</element>
                    <element>1.1.1.2/2</element>
               </BlackList>
               <CcEnabled>false</CcEnabled>
               <CcRuleEnabled>true</CcRuleEnabled>
               <CcTemplate>default</CcTemplate>
               <CertName>www_alibaba_com.pem</CertName>
               <Domain>www.alibaba.com</Domain>
               <ProxyTypeList>
                    <element>
                         <ProxyPorts>
                              <element>80</element>
                              <element>8080</element>
                         </ProxyPorts>
                         <ProxyType>http</ProxyType>
                    </element>
               </ProxyTypeList>
               <RealServers>
                    <element>
                         <RealServer>1.1.1.1</RealServer>
                         <RsType>0</RsType>
                    </element>
                    <element>
                         <RealServer>1.1.1.2</RealServer>
                         <RsType>1</RsType>
                    </element>
               </RealServers>
               <WhiteList>
                    <element>1.1.1.1/1</element>
                    <element>1.1.1.2/2</element>
               </WhiteList>
          </element>
          <element>
               <BlackList>
                    <element>1.1.1.1/1</element>
                    <element>1.1.1.2/2</element>
               </BlackList>
               <CcEnabled>false</CcEnabled>
               <CcRuleEnabled>true</CcRuleEnabled>
               <CcTemplate>default</CcTemplate>
               <CertName>www_alibaba_com.pem</CertName>
               <Domain>www.alibaba.com</Domain>
               <ProxyTypeList>
```

```
                    <element>
                        <ProxyPorts>
                            <element>80</element>
                            <element>8080</element>
                        </ProxyPorts>
                        <ProxyType>http</ProxyType>
                    </element>
                </ProxyTypeList>
                <RealServers>
                    <element>
                        <RealServer>1.1.1.1</RealServer>
                        <RsType>0</RsType>
                    </element>
                    <element>
                        <RealServer>1.1.1.2</RealServer>
                        <RsType>1</RsType>
                    </element>
                </RealServers>
                <WhiteList>
                    <element>1.1.1.1/1</element>
                    <element>1.1.1.2/2</element>
                </WhiteList>
            </element>
    </Domains>
    <RequestId>0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc</RequestId>
    <Total>2</Total>
</DescribeDomainsResponse>
```

JSON 格式

```
{
 "RequestId":"0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc",
 "Domains":[
  {
   "BlackList":[
    "1.1.1.1/1",
    "1.1.1.2/2"
   ],
   "Domain":"www.alibaba.com",
   "ProxyTypeList":[
    {
     "ProxyPorts":[
      80,
      8080
     ],
     "ProxyType":"http"
    }
   ],
   "RealServers":[
    {
     "RealServer":"1.1.1.1",
     "RsType":0
    },
    {
     "RealServer":"1.1.1.2",
     "RsType":1
    }
   ],
   "CcTemplate":"default",
   "CertName":"www_alibaba_com.pem",
   "CcRuleEnabled":true,
   "WhiteList":[
    "1.1.1.1/1",
```

```
      "1.1.1.2/2"
    ],
    "CcEnabled":false
   },
   {
    "BlackList":[
     "1.1.1.1/1",
     "1.1.1.2/2"
    ],
    "Domain":"www.alibaba.com",
    "ProxyTypeList":[
     {
      "ProxyPorts":[
       80,
       8080
      ],
      "ProxyType":"http"
     }
    ],
    "RealServers":[
     {
      "RealServer":"1.1.1.1",
      "RsType":0
     },
     {
      "RealServer":"1.1.1.2",
      "RsType":1
     }
    ],
    "CcTemplate":"default",
    "CertName":"www_alibaba_com.pem",
    "CcRuleEnabled":true,
    "WhiteList":[
     "1.1.1.1/1",
     "1.1.1.2/2"
    ],
    "CcEnabled":false
   }
  ],
  "Total":2
}
```


错误码

访问错误中心查看更多错误码。

5.6.2 CreateLayer7Rule

调用CreateLayer7Rule创建7层转发规则。

调试

您可以在*OpenAPI Explorer*中直接运行该接口，免去您计算签名的困扰。运行成功后，*OpenAPI Explorer*可以自动生成*SDK*代码示例。

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	CreateLayer7Rule	系统规定参数。取值：CreateLayer7Rule。
Domain	String	是	www.aliyun.com	要添加的域名。
RsType	Integer	是	0	源站类型，取值： · 0：IP · 1：域名
Rules	String	是	[{"ProxyRules":[{"ProxyPort":443,"RealServers":["1.1.1.1:443"]}],"ProxyType":"https"},{"ProxyRules":[{"ProxyPort":80,"RealServers":["1.1.1.1:80"]}],"ProxyType":"http"}]	传入7层规则Layer7Rule数组JSON串。具体结构描述如下： · ProxyRules，数组类型，必选，规则对象数组，包含以下元素： - ProxyPort，Integer类型，必选，协议端口，取值：80、443。 - RealServers，String类型，必选，用户源站。例如，1.1.1.1:443。 · ProxyType，String类型，必选，协议类型，取值：http、https、websocket、websockets。
InstanceIds.N	RepeatList	否	ddoscoo-cn-XXXXX	要绑定的实例ID。若有多个实例，依次传入InstanceIds.1, InstanceIds.2, InstanceIds.3, .. 说明: 若不传入该参数，则只添加域名，不绑定到具体IP。
ResourceGroupId	String	否	test	资源组ID。

返回数据

名称	类型	示例值	描述
RequestId	String	CF33B4C3-196E-4015-AADD-5CAD00057B80	本次请求的ID。

示例

请求示例

```
http(s)://[Endpoint]/?Action=CreateLayer7Rule
&Domain=www.aliyun.com
&RsType=0
&Rules=[{"ProxyRules":[{"ProxyPort":443,"RealServers":["1.1.1.1:443
"]}],"ProxyType":"https"},{"ProxyRules":[{"ProxyPort":80,"RealServers
":["1.1.1.1:80"]}],"ProxyType":"http"}]
&<公共请求参数>
```

正常返回示例

`XML` **格式**

```
<CreateLayer7RuleResponse>
      <RequestId>0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc</RequestId>
</CreateLayer7RuleResponse>
```

`JSON` **格式**

```
{
 "RequestId":"0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc"
}
```

错误码

访问**错误中心**查看更多错误码。

5.6.3 ConfigLayer7Rule

调用ConfigLayer7Rule编辑7层转发规则。

调试

您可以在*OpenAPI Explorer*中直接运行该接口，免去您计算签名的困扰。运行成功后，*OpenAPI Explorer*可以自动生成*SDK*代码示例。

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	ConfigLayer7Rule	系统规定参数。取值：ConfigLayer7Rule。
Domain	String	是	www.aliyun.com	要操作的域名。
RealServers.N	RepeatList	是	1.1.1.1	源站IP。若有多个源站IP，依次传入RealServers.1, RealServers.2, RealServers.3, ...
RsType	Integer	是	0	源站类型，取值： · 0：IP · 1：域名
InstanceIds.N	RepeatList	否	ddoscoo-cn-XXXXXX	要绑定的实例Id。若有多个实例，依次传入InstanceIds.1, InstanceIds.2, InstanceIds.3, ... 说明: 若不传入该参数，则只添加域名，不绑定到具体IP。
ProxyTypeList	String	否	[{"ProxyPorts":[80,8080],"ProxyType":"http"},{"ProxyPorts":[443],"ProxyType":"https"}]rts\":[443],\"ProxyType\":\"https\"}]	协议数组。具体结构描述如下： · ProxyType，String类型，必选，协议类型，取值：http、https、websocket、websockets。 · ProxyPorts，Integer类型，必选，协议端口。
ResourceGroupId	String	否	test	资源组ID。

返回数据

名称	类型	示例值	描述
RequestId	String	CF33B4C3-196E-4015-AADD-5CAD00057B80	本次请求的ID。

示例

请求示例

```
http(s)://[Endpoint]/?Action=ConfigLayer7Rule
&Domain=www.aliyun.com
&RealServers.1=1.1.1.1
&RsType=0
&<公共请求参数>
```

正常返回示例

`XML` **格式**

```
<ConfigLayer7RuleResponse>
     <RequestId>0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc</RequestId>
</ConfigLayer7RuleResponse>
```

`JSON` **格式**

```
{
 "RequestId":"0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc"
}
```

错误码

访问错误中心查看更多错误码。

5.6.4 DeleteLayer7Rule

调用DeleteLayer7Rule删除7层转发规则。

调试

您可以在*OpenAPI Explorer*中直接运行该接口，免去您计算签名的困扰。运行成功后，*OpenAPI Explorer*可以自动生成*SDK*代码示例。

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	DeleteLayer7Rule	系统规定参数。取值：DeleteLayer7Rule。
Domain	String	是	www.aliyun.com	要操作的域名。
ResourceGroupId	String	否	test	资源组ID。

返回数据

名称	类型	示例值	描述
RequestId	String	CF33B4C3-196E-4015-AADD-5CAD00057B80	本次请求的ID。

示例

请求示例

```
http(s)://[Endpoint]/?Action=DeleteLayer7Rule
&Domain=www.aliyun.com
&<公共请求参数>
```

正常返回示例

`XML` **格式**

```
<DeleteLayer7RuleResponse>
      <RequestId>0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc</RequestId>
</DeleteLayer7RuleResponse>
```

`JSON` **格式**

```
{
 "RequestId":"0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc"
}
```

错误码

访问错误中心查看更多错误码。

5.6.5 ConfigLayer7Cert

调用ConfigLayer7Cert为指定域名配置7层证书。

设置证书。新BGP高防的证书上传功能已接入云盾证书服务，您可以直接调用该接口从证书服务拉取对应的证书上传到新BGP高防服务。当您选择重新上传一组证书和私钥时，我们会将您的这组证书和私钥重新上传到云盾证书服务，以便您可以重复使用这组证书。

调试

您可以在*OpenAPI Explorer*中直接运行该接口，免去您计算签名的困扰。运行成功后，*OpenAPI Explorer*可以自动生成*SDK*代码示例。

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	ConfigLayer7Cert	系统规定参数。取值：ConfigLayer7Cert。
Domain	String	是	www.aliyun.com	要操作的域名。
Cert	String	否	xx	证书公钥。 说明: 若传入此参数，则必须同时传入CertName和Key。若传入CertName、Cert、Key组合，则无需传入CertId。
CertId	Integer	否	1234	证书ID。 说明: 若传入此参数，则无需传入CertName、Cert、Key。
CertName	String	否	testCertName	证书名称。 说明: 若传入此参数，则必须同时传入Cert和Key。若传入CertName、Cert、Key组合，则无需传入CertId。

名称	类型	是否必选	示例值	描述
Key	String	否	xx	证书私钥。 说明: 若传入此参数，则必须同时传入CertName和Cert。若传入CertName、Cert、Key组合，则无需传入CertId。
ResourceGroupId	String	否	xx	资源组ID。

返回数据

名称	类型	示例值	描述
RequestId	String	0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc	本次请求的ID。

示例

请求示例

```
http(s)://[Endpoint]/?Action=ConfigLayer7Cert
&Domain=www.aliyun.com
&CertId=1
&<公共请求参数>
```

正常返回示例

`XML` **格式**

```
<ConfigLayer7CertResponse>
     <RequestId>0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc</RequestId>
</ConfigLayer7CertResponse>
```

`JSON` **格式**

```
{
 "RequestId":"0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc"
}
```

错误码

访问错误中心查看更多错误码。

5.6.6 ConfigLayer7BlackWhiteList

调用ConfigLayer7BlackWhiteList为指定域名设置7层防护黑白名单。

调试

您可以在*OpenAPI Explorer*中直接运行该接口，免去您计算签名的困扰。运行成功后，*OpenAPI Explorer*可以自动生成*SDK*代码示例。

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	ConfigLayer7BlackWhiteList	系统规定参数。取值：ConfigLayer7BlackWhiteList。
Domain	String	是	www.aliyun.com	要配置的域名。
BlackList.N	RepeatList	否	1.1.1.1	黑名单列表。若有多个加黑地址，依次传入BlackList.1, BlackList.2, BlackList.3, ...
ResourceGroupId	String	否	test	资源组ID。
WhiteList.N	RepeatList	否	1.1.1.1	白名单列表。若有多个加白地址，依次传入WhiteList.1, WhiteList.2, WhiteList.3, ...

返回数据

名称	类型	示例值	描述
RequestId	String	CF33B4C3-196E-4015-AADD-5CAD00057B80	本次请求的ID。

示例

请求示例

```
http(s)://[Endpoint]/?Action=ConfigLayer7BlackWhiteList
&Domain=www.aliyun.com
```

```
&<公共请求参数>
```

正常返回示例

`XML` **格式**

```
<ConfigLayer7BlackWhiteListResponse>
      <RequestId>0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc</RequestId>
</ConfigLayer7BlackWhiteListResponse>
```

`JSON` **格式**

```
{
 "RequestId":"0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc"
}
```

错误码

访问错误中心查看更多错误码。

5.6.7 DescribleLayer7InstanceRelations

调用DescribleLayer7InstanceRelations查询七层防护实例和EIP的对应关系。

调试

您可以在*OpenAPI Explorer*中直接运行该接口，免去您计算签名的困扰。运行成功后，*OpenAPI Explorer*可以自动生成*SDK*代码示例。

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	DescribleLayer7InstanceRelations	系统规定参数。取值：DescribleLayer7InstanceRelations。
DomainList.N	RepeatLis	是	www.aliyun.com	要查询的域名列表。
ResourceGroupId	String	否	test	资源组ID。

返回数据

名称	类型	示例值	描述
Layer7InstanceRelations			七层实例的防护关系列表。

名称	类型	示例值	描述
Domain	String	www.aliyun.com	域名。
InstanceDetails			实例信息列表。
EipList		["203.107.0.0"]	绑定的EIP列表。
FunctionVersion	String	default	功能版本，取值： · default：标准版 · enhance：增强版
InstanceId	String	ddoscoo-cn-XXXXX	实例ID
RequestId	String	CF33B4C3-196E-4015-AADD-5CAD00057B80	本次请求的ID。

示例

请求示例

```
http(s)://[Endpoint]/?Action=DescribleLayer7InstanceRelations
&DomainList.1=www.aliyun.com
&<公共请求参数>
```

正常返回示例

`XML` **格式**

```
<DescribleLayer7InstanceRelationsResponse>
     <Layer7InstanceRelations>
          <element>
               <Domain>1.aliyun.com</Domain>
               <InstanceDetails>
                    <element>
                         <EipList>
                              <element>203.x.x.0</element>
                              <element>203.x.x.1</element>
                         </EipList>
                         <InstanceId>xxxxxx</InstanceId>
                    </element>
                    <element>
                         <EipList>
                              <element>203.x.x.0</element>
                              <element>203.x.x.1</element>
                         </EipList>
                         <FunctionVersion>default</FunctionVersion>
                         <InstanceId>xxxxxx</InstanceId>
                    </element>
```

```
                </InstanceDetails>
            </element>
        </Layer7InstanceRelations>
</DescribleLayer7InstanceRelationsResponse>
```

JSON 格式

```
{
 "Layer7InstanceRelations":[
  {
   "InstanceDetails":[
    {
     "FunctionVersion":"default",
     "InstanceId":"xxxxxx",
     "EipList":[
      "203.x.x.0",
      "203.x.x.1"
     ]
    },
    {
     "InstanceId":"xxxxxx",
     "EipList":[
      "203.x.x.0",
      "203.x.x.1"
     ]
    }
   ],
   "Domain":"1.aliyun.com"
  }
 ]
}
```

错误码

访问错误中心查看更多错误码。

5.6.8 DescribleCertList

调用DescribleCertList查询所有证书列表。

调试

您可以在*OpenAPI Explorer*中直接运行该接口，免去您计算签名的困扰。运行成功后，*OpenAPI Explorer*可以自动生成*SDK*代码示例。

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	DescribleCertList	系统规定参数。取值：DescribleCertList。
ResourceGroupId	String	否	test	资源组ID。

返回数据

名称	类型	示例值	描述
CertList			证书列表。
Id	Integer	123	证书ID。
Name	String	testCertName	证书名称。
RequestId	String	CF33B4C3-196E-4015-AADD-5CAD00057B80	本次请求的ID。

示例

请求示例

```
http(s)://[Endpoint]/?Action=DescribleCertList
&<公共请求参数>
```

正常返回示例

`XML` **格式**

```
<DescribleCertListResponse>
     <RequestId>CF33B4C3-196E-4015-AADD-5CAD00057B80</RequestId>
</DescribleCertListResponse>
```

`JSON` **格式**

```
{
 "RequestId":"CF33B4C3-196E-4015-AADD-5CAD00057B80"
}
```

错误码

访问**错误中心**查看更多错误码。

5.6.9 EnableLayer7CC

调用EnableLayer7CC为指定域名启用7层CC防护。

调试

您可以在*OpenAPI Explorer*中直接运行该接口，免去您计算签名的困扰。运行成功后，*OpenAPI Explorer*可以自动生成*SDK*代码示例。

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	EnableLayer7CC	系统规定参数。取值：EnableLayer7CC。
Domain	String	是	www.aliyun.com	要操作的域名。
ResourceGroupId	String	否	test	资源组ID。

返回数据

名称	类型	示例值	描述
RequestId	String	CF33B4C3-196E-4015-AADD-5CAD00057B80	本次请求的ID。

示例

请求示例

```
http(s)://[Endpoint]/?Action=EnableLayer7CC
&Domain=www.aliyun.com
&<公共请求参数>
```

正常返回示例

`XML` **格式**

```
<EnableLayer7CCResponse>
      <RequestId>0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc</RequestId>
</EnableLayer7CCResponse>
```

`JSON` **格式**

```
{
 "RequestId":"0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc"
}
```

错误码

访问错误中心查看更多错误码。

5.6.10 DisableLayer7CC

调用DisableLayer7CC为指定域名禁用7层CC防护。

调试

您可以在*OpenAPI Explorer*中直接运行该接口，免去您计算签名的困扰。运行成功后，*OpenAPI Explorer*可以自动生成*SDK*代码示例。

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	DisableLayer7CC	系统规定参数。取值：DisableLayer7CC。
Domain	String	是	www.aliyun.com	要操作的域名。
ResourceGroupId	String	否	test	资源组ID。

返回数据

名称	类型	示例值	描述
RequestId	String	CF33B4C3-196E-4015-AADD-5CAD00057B80	本次请求的ID。

示例

请求示例

```
http(s)://[Endpoint]/?Action=DisableLayer7CC
&Domain=www.aliyun.com
&<公共请求参数>
```

正常返回示例

`XML` **格式**

```
<DisableLayer7CCResponse>
      <RequestId>0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc</RequestId>
</DisableLayer7CCResponse>
```

`JSON` **格式**

```
{
 "RequestId":"0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc"
```

```
}
```

错误码

访问错误中心查看更多错误码。

5.6.11 EnableLayer7CCRule

调用EnableLayer7CCRule为指定域名启用7层CC规则。

调试

您可以在*OpenAPI Explorer*中直接运行该接口，免去您计算签名的困扰。运行成功后，*OpenAPI Explorer*可以自动生成*SDK*代码示例。

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	EnableLayer7CCRule	系统规定参数。取值：EnableLayer7CCRule。
Domain	String	是	www.aliyun.com	要操作的域名。
ResourceGroupId	String	否	test	资源组ID。

返回数据

名称	类型	示例值	描述
RequestId	String	CF33B4C3-196E-4015-AADD-5CAD00057B80	本次请求的ID。

示例

请求示例

```
http(s)://[Endpoint]/?Action=EnableLayer7CCRule
&Domain=www.aliyun.com
&<公共请求参数>
```

正常返回示例

XML 格式

```
<EnableLayer7CCRuleResponse>
      <RequestId>0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc</RequestId>
```

```
</EnableLayer7CCRuleResponse>
```

JSON 格式

```
{
 "RequestId":"0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc"
}
```

错误码

访问错误中心查看更多错误码。

5.6.12 DisableLayer7CCRule

调用DisableLayer7CCRule为指定域名禁用7层CC规则。

调试

您可以在*OpenAPI Explorer*中直接运行该接口，免去您计算签名的困扰。运行成功后，*OpenAPI Explorer*可以自动生成*SDK*代码示例。

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	DisableLayer7CCRule	系统规定参数。取值：DisableLayer7CCRule。
Domain	String	是	www.aliyun.com	要操作的域名。
ResourceGroupId	String	否	test	资源组ID。

返回数据

名称	类型	示例值	描述
RequestId	String	CF33B4C3-196E-4015-AADD-5CAD00057B80	本次请求的ID。

示例

请求示例

```
http(s)://[Endpoint]/?Action=DisableLayer7CCRule
&Domain=www.aliyun.com
```

```
&<公共请求参数>
```

正常返回示例

XML 格式

```
<DisableLayer7CCRuleResponse>
     <RequestId>0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc</RequestId>
</DisableLayer7CCRuleResponse>
```

JSON 格式

```
{
 "RequestId":"0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc"
}
```

错误码

访问错误中心查看更多错误码。

5.6.13 AddLayer7CCRule

调用AddLayer7CCRule为指定域名添加7层CC规则。

调试

您可以在*OpenAPI Explorer*中直接运行该接口，免去您计算签名的困扰。运行成功后，*OpenAPI Explorer*可以自动生成*SDK*代码示例。

请求参数

名称	类型	是否必选	示例值	描述
Act	String	是	close	规则触发后的操作，取值： · close：封禁 · captcha：人机识别
Action	String	是	AddLayer7CCRule	系统规定参数。取值：AddLayer7CCRule。
Count	Integer	是	2	访问次数，与Interval结和使用。当同一个IP在Interval指定的间隔时间内连续访问Count中指定的访问次数，则触发规则。取值范围为2~2,000。

名称	类型	是否必选	示例值	描述
Domain	String	是	www.aliyun.com	要操作的域名。
Interval	Integer	是	5	间隔时间，与Count结和使用。当同一个IP在Interval指定的间隔时间内连续访问Count中指定的访问次数，则触发规则。取值范围为5~10,800。
Mode	String	是	match	URI匹配模式，取值： · match：完全匹配。访问请求的URI与指定的Uri完全相同，才计入访问次数。 · prefix：前缀匹配。访问请求的URI包含指定的Uri，则计入访问次数。
Name	String	是	testCcRule1	CC自定义规则名。
Ttl	Integer	是	60	若规则触发后动作指定为封禁，设置封禁时间，单位为秒，取值范围为60~86,400。
Uri	String	是	/a/b/c	被防护的URI。
ResourceGroupId	String	否	test	资源组ID。

返回数据

名称	类型	示例值	描述
RequestId	String	CF33B4C3-196E-4015-AADD-5CAD00057B80	本次请求的ID。

示例

请求示例

```
http(s)://[Endpoint]/?Action=AddLayer7CCRule
&Act=close
```

```
&Count=2
&Domain=www.aliyun.com
&Interval=5
&Mode=match
&Name=testCcRule1
&Ttl=60
&Uri=/a/b/c
&<公共请求参数>
```

正常返回示例

XML 格式

```
<AddLayer7CCRuleResponse>
     <RequestId>0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc</RequestId>
</AddLayer7CCRuleResponse>
```

JSON 格式

```
{
 "RequestId":"0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc"
}
```

错误码

访问错误中心查看更多错误码。

5.6.14 ConfigLayer7CCRule

调用ConfigLayer7CCRule编辑7层CC规则。

调试

您可以在*OpenAPI Explorer*中直接运行该接口，免去您计算签名的困扰。运行成功后，*OpenAPI Explorer*可以自动生成*SDK*代码示例。

请求参数

名称	类型	是否必选	示例值	描述
Act	String	是	close	规则触发后的操作，取值： · close：封禁 · captcha：人机识别
Action	String	是	ConfigLayer7CCRule	系统规定参数。取值：ConfigLayer7CCRule。

名称	类型	是否必选	示例值	描述
Count	Integer	是	2	访问次数，与Interval结和使用。当同一个IP在Interval指定的间隔时间内连续访问Count中指定的访问次数，则触发规则。取值范围为2~2,000。
Domain	String	是	www.aliyun.com	要操作的域名。
Interval	Integer	是	5	间隔时间，与Count结和使用。当同一个IP在Interval指定的间隔时间内连续访问Count中指定的访问次数，则触发规则。取值范围为5~10,800。
Mode	String	是	match	URI匹配模式，取值： · match：完全匹配。访问请求的URI与指定的Uri完全相同，才计入访问次数。 · prefix：前缀匹配。访问请求的URI包含指定的Uri，则计入访问次数。
Name	String	是	testCcRule1	CC自定义规则名。
Ttl	Integer	是	60	若规则触发后动作指定为封禁，设置封禁时间，单位为秒，取值范围为60~86,400。
Uri	String	是	/a/b/c	被防护的URI。
ResourceGroupId	String	否	test	资源组ID。

返回数据

名称	类型	示例值	描述
RequestId	String	CF33B4C3-196E-4015-AADD-5CAD00057B80	本次请求的ID。

示例

请求示例

```
http(s)://[Endpoint]/?Action=ConfigLayer7CCRule
&Act=close
&Count=2
&Domain=www.aliyun.com
&Interval=5
&Mode=match
&Name=testCcRule1
&Ttl=60
&Uri=/a/b/c
&<公共请求参数>
```

正常返回示例

`XML` **格式**

```
<ConfigLayer7CCRuleResponse>
      <RequestId>0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc</RequestId>
</ConfigLayer7CCRuleResponse>
```

`JSON` **格式**

```
{
 "RequestId":"0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc"
}
```

错误码

访问错误中心查看更多错误码。

5.6.15 DescribeLayer7CCRules

调用DescribeLayer7CCRules查询7层CC规则。

调试

您可以在*OpenAPI Explorer*中直接运行该接口，免去您计算签名的困扰。运行成功后，*OpenAPI Explorer*可以自动生成*SDK*代码示例。

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	DescribeLayer7CCRules	系统规定参数。取值：DescribeLayer7CCRules。
Domain	String	是	www.aliyun.com	要查询的域名。
Offset	Integer	是	0	开始索引位置，即从第几个结果开始返回。 说明: 若不传入该参数，则从第0个结果开始返回。
PageSize	String	是	10	分页大小，即每页显示过少个结果。最大值10。
ResourceGroupId	String	否	test	资源组ID。

返回数据

名称	类型	示例值	描述
Layer7CCRules			CC规则数组。
Act	String	close	规则触发后的操作，取值： · close：封禁 · captcha：人机识别
Count	Integer	100	访问次数，与Interval结和使用。当同一个IP在Interval指定的间隔时间内连续访问Count中指定的访问次数，则触发规则。

名称	类型	示例值	描述
Interval	Integer	60	间隔时间，与Count结和使用。当同一个IP在Interval指定的间隔时间内连续访问Count中指定的访问次数，则触发规则。
Mode	String	match	URI匹配模式，取值： · match：完全匹配。访问请求的URI与指定的Uri完全相同，才计入访问次数。 · prefix：前缀匹配。访问请求的URI包含指定的Uri，则计入访问次数。
Name	String	testCcRule1	CC自定义规则名。
Ttl	Integer	1000	若规则触发后动作指定为封禁，设置封禁时间。
Uri	String	/a/b/c	被防护的URI。
RequestId	String	CF33B4C3-196E-4015-AADD-5CAD00057B80	本次请求的ID。
Total	Long	10	规则总数。

示例

请求示例

```
http(s)://[Endpoint]/?Action=DescribeLayer7CCRules
&Domain=www.aliyun.com
&Offset=0
&PageSize=10
&<公共请求参数>
```

正常返回示例

`XML` **格式**

```
<DescribeLayer7CCRulesResponse>
     <Layer7CCRules>
          <element>
```

```
                <Act>close</Act>
                <Count>11</Count>
                <Interval>5</Interval>
                <Mode>match</Mode>
                <Name>XXXX</Name>
                <Ttl>1</Ttl>
                <Uri>/a/b/c.htm</Uri>
          </element>
          <element>
                <Act>close</Act>
                <Count>11</Count>
                <Interval>5</Interval>
                <Mode>match</Mode>
                <Name>XXXX</Name>
                <Ttl>1</Ttl>
                <Uri>/a/b/c.htm</Uri>
          </element>
     </Layer7CCRules>
     <RequestId>0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc</RequestId>
     <Total>10</Total>
</DescribeLayer7CCRulesResponse>
```

JSON 格式

```
{
 "RequestId":"0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc",
 "Layer7CCRules":[
  {
   "Name":"XXXX",
   "Interval":5,
   "Count":11,
   "Act":"close",
   "Ttl":1,
   "Uri":"/a/b/c.htm",
   "Mode":"match"
  },
  {
   "Name":"XXXX",
   "Interval":5,
   "Count":11,
   "Act":"close",
   "Ttl":1,
   "Uri":"/a/b/c.htm",
   "Mode":"match"
  }
 ],
 "Total":10
}
```

错误码

访问错误中心查看更多错误码。

5.6.16 DeleteLayer7CCRule

调用DeleteLayer7CCRule删除7层CC规则。

调试

您可以在*OpenAPI Explorer*中直接运行该接口，免去您计算签名的困扰。运行成功后，*OpenAPI Explorer*可以自动生成*SDK*代码示例。

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	DeleteLayer7CCRule	系统规定参数。取值：DeleteLayer7CCRule。
Domain	String	是	www.aliyun.com	要操作的域名。
Name	String	是	testCcRule1	要删除的CC自定义规则名。
ResourceGroupId	String	否	test	资源组ID。

返回数据

名称	类型	示例值	描述
RequestId	String	CF33B4C3-196E-4015-AADD-5CAD00057B80	本次请求的ID。

示例

请求示例

```
http(s)://[Endpoint]/?Action=DeleteLayer7CCRule
&Domain=www.aliyun.com
&Name=testCcRule1
&<公共请求参数>
```

正常返回示例

XML 格式

```
<DeleteLayer7CCRuleResponse>
      <RequestId>0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc</RequestId>
```

```
</DeleteLayer7CCRuleResponse>
```

JSON 格式

```
{
 "RequestId":"0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc"
}
```

错误码

访问错误中心查看更多错误码。

5.6.17 ConfigLayer7CCTemplate

调用ConfigLayer7CCTemplate为指定域名设置7层CC防护模式。

调试

您可以在*OpenAPI Explorer*中直接运行该接口，免去您计算签名的困扰。运行成功后，*OpenAPI Explorer*可以自动生成*SDK*代码示例。

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	ConfigLayer7CCTemplate	系统规定参数。取值：ConfigLayer7CCTemplate。
Domain	String	是	www.aliyun.com	要操作的域名。
Template	String	是	default	要应用的CC防护模式，取值： · default：正常 · gf_under_attack：攻击紧急 · gf_sos_verify：严格 · gf_sos_enhance：超级严格
ResourceGroupId	String	否	test	资源组ID。

返回数据

名称	类型	示例值	描述
RequestId	String	CF33B4C3-196E-4015-AADD-5CAD00057B80	本次请求的ID。

示例

请求示例

```
http(s)://[Endpoint]/?Action=ConfigLayer7CCTemplate
&Domain=www.aliyun.com
&Template=default
&<公共请求参数>
```

正常返回示例

`XML` **格式**

```
<ConfigLayer7CCTemplateResponse>
      <RequestId>0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc</RequestId>
</ConfigLayer7CCTemplateResponse>
```

`JSON` **格式**

```
{
 "RequestId":"0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc"
}
```

错误码

访问错误中心查看更多错误码。

5.6.18 DescribeDomainAccessMode

调用DescribeDomainAccessMode查询域名的接入模式。

调试

您可以在*OpenAPI Explorer*中直接运行该接口，免去您计算签名的困扰。运行成功后，*OpenAPI Explorer*可以自动生成*SDK*代码示例。

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	DescribeDomainAccessMode	系统规定参数。取值：DescribeDomainAccessMode。
DomainList.N	RepeatLis	是	www.aliyun.com	要查询的域名。所有多个域名，依次传入DomainList.1, DomainList.2, DomainList.3, ...

返回数据

名称	类型	示例值	描述
DomainModeList			模式配置。
AccessMode	Integer	1	接入模式，取值： · 0：A记录 · 1：高防 · 2：回源
Domain	String	www.aliyun.com	域名。
RequestId	String	CF33B4C3-196E-4015-AADD-5CAD00057B80	本次请求的ID。

示例

请求示例

```
http(s)://[Endpoint]/?Action=DescribeDomainAccessMode
&DomainList.1=www.aliyun.com
&<公共请求参数>
```

正常返回示例

`XML` **格式**

```
<DescribeDomainAccessModeResponse>
     <DomainModeList>
          <element>
               <AccessMode>1</AccessMode>
               <Domain>www.alibaba.com</Domain>
          </element>
          <element>
               <AccessMode>2</AccessMode>
               <Domain>www.aliyun.com</Domain>
          </element>
     </DomainModeList>
     <RequestId>0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc</RequestId>
</DescribeDomainAccessModeResponse>
```

`JSON` **格式**

```
{
 "RequestId":"0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc",
 "DomainModeList":[
  {
   "AccessMode":1,
```

```
    "Domain":"www.alibaba.com"
   },
   {
    "AccessMode":2,
    "Domain":"www.aliyun.com"
   }
  ]
}
```

错误码

访问错误中心查看更多错误码。

5.6.19 ConfigDomainAccessMode

调用ConfigDomainAccessMode设置域名接入模式。

调试

您可以在*OpenAPI Explorer*中直接运行该接口，免去您计算签名的困扰。运行成功后，*OpenAPI Explorer*可以自动生成*SDK*代码示例。

请求参数

名称	类型	是否必选	示例值	描述
AccessMode	Integer	是	2	接入模式，取值： · 0：A记录 · 1：高防 · 2：回源
Action	String	是	ConfigDomainAccessMode	系统规定参数。取值：ConfigDomainAccessMode。
Domain	String	是	www.aliyun.com	要操作的域名。

返回数据

名称	类型	示例值	描述
RequestId	String	CF33B4C3-196E-4015-AADD-5CAD00057B80	本次请求的ID。

示例

请求示例

```
http(s)://[Endpoint]/?Action=ConfigDomainAccessMode
&AccessMode=2
&Domain=www.aliyun.com
&<公共请求参数>
```

正常返回示例

`XML` **格式**

```
<ConfigDomainAccessModeResponse>
     <RequestId>0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc</RequestId>
</ConfigDomainAccessModeResponse>
```

`JSON` **格式**

```
{
 "RequestId":"0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc"
}
```

错误码

访问错误中心查看更多错误码。

5.6.20 DescribeBackSourceCidr

调用DescribeBackSourceCidr查询回源网段。

调试

您可以在*OpenAPI Explorer*中直接运行该接口，免去您计算签名的困扰。运行成功后，*OpenAPI Explorer*可以自动生成*SDK*代码示例。

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	DescribeBackSourceCidr	系统规定参数。取值：DescribeBackSourceCidr。
Line	String	否	coop-line-001	要查询的防护线路。
ResourceGroupId	String	否	test	资源组ID。

返回数据

名称	类型	示例值	描述
CidrList		["47.97.128.0/25","47.97.128.128/25"]	回源IP段列表。
RequestId	String	CF33B4C3-196E-4015-AADD-5CAD00057B80	本次请求的ID。

示例

请求示例

```
http(s)://[Endpoint]/?Action=DescribeBackSourceCidr
&Line=coop-line-001
&<公共请求参数>
```

正常返回示例

`XML` **格式**

```
<DescribeBackSourceCidrResponse>
      <CidrList>
            <element>47.xx.xx.0/25</element>
            <element>47.xx.xx.128/25</element>
      </CidrList>
      <RequestId>0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc</RequestId>
</DescribeBackSourceCidrResponse>
```

`JSON` **格式**

```
{
 "RequestId":"0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc",
 "CidrList":[
  "47.xx.xx.0/25",
  "47.xx.xx.128/25"
 ]
}
```

错误码

访问错误中心查看更多错误码。

5.7 事件任务

5.7.1 ListAsyncTask

调用ListAsyncTask查询异步任务列表。

请求参数

名称	类型	是否必需	描述
TaskType	Integer	否	要查询的任务类型，取值： · 1：4层转发规则批量导出任务 · 2：7层防护规则批量导出任务 · 3：会话&健康检查配置导出任务 · 4：DDoS防护策略导出任务 说明: 若不传入该参数，则返回所有类型的任务。
TaskStatus	Integer	否	要查询的任务状态，取值： · 0：任务初始化 · 1：任务进行中 · 2：任务成功 · 3：任务失败 说明: 若不传入该参数，则返回所有状态的任务。
PageNo	Integer	是	当前页数，从1开始。
PageSize	Integer	是	分页大小，最大值20。

返回参数

名称	类型	描述
RequestId	String	本次请求的ID。
Total	Integer	域名总数。
AsyncTasks	[] AsyncTask	任务列表。具体结构描述见*AsyncTask*。

表 5-3: AsyncTask

名称	类型	描述
TaskId	Long	任务ID，使用该ID可进行任务的删除操作。

名称	类型	描述
TaskType	Integer	任务类型，取值： · 1：4层转发规则批量导出任务 · 2：7层防护规则批量导出任务 · 3：会话&健康检查配置导出任务 · 4：DDoS防护策略导出任务
TaskStatus	Integer	任务状态，取值： · 0：任务初始化 · 1：任务进行中 · 2：任务成功 · 3：任务失败
StartTime	Long	任务开始时间戳，单位：毫秒。
EndTime	Long	任务结束时间戳，单位：毫秒。
TaskParams	TaskParam	任务执行参数，为一个JSONObject类型的字符串，具体结构描述见*TaskParam*。
TaskResult	TaskResult	任务执行结果，JSONObject类型的字符串，具体结构描述见*TaskResult*。

表 5-4: TaskParam

名称	类型	描述
instanceId	String	新BGP高防实例ID。
domain	String	用户域名。

表 5-5: TaskResult

名称	类型	描述
instanceId	String	新BGP高防实例ID。
url	String	文件下载OSS地址。

示例

请求示例

```
{
  "TaskType": 1,
  "TaskStatus": 0,
  "PageNo":1,
```

```
  "PageSize":10
}
```

返回示例

```
{
  "Total": 2,
  "RequestId": "0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc",
  "AsyncTasks": [
   {
  "TaskId": 1,
     "TaskType": 1,
     "TaskStatus": 2,
     "StartTime": 156927362,
   "EndTime": 156927362
     "TaskParams": "{}", // 四层任务：{"instanceId": "ddoscoo-1234-
qrq2134"}，七层任务：{"domain": "www.aliyun.com"}
       "TaskResult": "{}" // 四层任务：{"instanceId": "ddoscoo-1234-
qrq2134", "url": "https://oss.xxx.xxx"}，七层任务：{"domain": "www.aliyun
.com", "url": "https://oss.xxx.xxx"}，会话&健康检查任务：{"instanceId": "
ddoscoo-1234-qrq2134", "url": "https://oss.xxx.xxx"}，DDoS防护策略任务：
{"instanceId": "ddoscoo-1234-qrq2134", "url": "https://oss.xxx.xxx"}
 }
  ]
}
```

5.7.2 CreateAsyncTask

调用CreateAsyncTask创建异步任务。

请求参数

名称	类型	是否必需	描述
TaskType	Integer	是	任务类型，取值： · 1：4层转发规则批量导出任务 · 2：7层防护规则批量导出任务 · 3：会话&健康检查配置导出任务 · 4：DDoS防护策略导出任务

名称	类型	是否必需	描述
TaskParams	String	是	任务参数，一组json字符串，根据TaskType不同有所区别。 • TaskType为1时，传入需要导出规则的新BGP高防实例Id。例如，{“instanceId”: “ddoscoo-cn-XXXXX”} • TaskType为2时，传入一个空对象的字符串即可。例如，{} • TaskType为3时，传入需要导出规则的新BGP高防实例Id。例如，{“instanceId”: “ddoscoo-cn-XXXXX”} • TaskType为4时，传入需要导出规则的新BGP高防实例Id。例如，{“instanceId”: “ddoscoo-cn-XXXXX”}

返回参数

名称	类型	描述
RequestId	String	本次请求的ID。

示例

请求示例

```
{
  "TaskType": 1,
  "TaskParams": "{}" // 四层任务：{"instanceId": "ddoscoo-woieuroi234"}，七层任务：{}，会话&健康检查任务：{"instanceId": "xxxxxxxxxx"}，DDoS防护策略任务：{"instanceId": "xxxxxxxxxx"}
}
```

返回示例

```
{
  "RequestId": "0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc"
}
```

5.7.3 DeleteAsyncTask

调用DeleteAsyncTask删除指定的异步任务。

调试

您可以在*OpenAPI Explorer*中直接运行该接口，免去您计算签名的困扰。运行成功后，*OpenAPI Explorer*可以自动生成*SDK*代码示例。

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	DeleteAsyncTask	系统规定参数。取值：DeleteAsyncTask。
TaskId	Integer	是	123	要删除的任务ID。
ResourceGroupId	String	否	test	资源组ID。

返回数据

名称	类型	示例值	描述
RequestId	String	CF33B4C3-196E-4015-AADD-5CAD00057B80	本次请求的ID。

示例

请求示例

```
http(s)://[Endpoint]/?Action=DeleteAsyncTask
&TaskId=123
&<公共请求参数>
```

正常返回示例

`XML` **格式**

```
<DeleteAsyncTaskResponse>
     <RequestId>0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc</RequestId>
</DeleteAsyncTaskResponse>
```

`JSON` **格式**

```
{
 "RequestId":"0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc"
}
```

错误码

访问错误中心查看更多错误码。

5.8 日志

5.8.1 DescribeOpEntities

调用DescribeOpEntities查询操作日志。

调试

您可以在*OpenAPI Explorer*中直接运行该接口，免去您计算签名的困扰。运行成功后，*OpenAPI Explorer*可以自动生成*SDK*代码示例。

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	DescribeOpEntities	系统规定参数。取值：DescribeOpEntities。
EndTime	Long	是	1536715558000	结束时间时间戳，单位：毫秒。
PageNo	Integer	是	1	页号，即从第几页开始显示。
PageSize	Integer	是	10	分页大小，即每页显示多少条结果。最大值50。
StartTime	Long	是	1534123558000	开始时间时间戳，单位：毫秒。
ResourceGroupId	String	否	test	资源组ID。

返回数据

名称	类型	示例值	描述
OpEntities			操作日志。
EntityObject	String	2.2.2.2	操作对象的值，即操作的IP地址。
EntityType	Integer	1	操作对象类型。取值：1（IP类型）。
GmtCreate	Long	1536715558000	创建日志的时间戳，单位：毫秒。
OpAccount	String	123	操作人。
OpAction	Integer	1	操作类型。取值：1（修改弹性带宽）。

名称	类型	示例值	描述
OpDesc	String	{"newEntity":{"elasticBandwidth":30},"oldEntity":{"elasticBandwidth":200}}	操作详情。OpDesc的JSON字符串，具体结构描述如下： · oldValue，Struct类型，旧值，具体结构描述如下： - elasticBandwidth，Integer类型，弹性带宽值。 · newValue，Struct类型，新值，具体结构描述如下： - elasticBandwidth，Integer类型，弹性带宽值。
RequestId	String	CF33B4C3-196E-4015-AADD-5CAD00057B80	本次请求的ID。
Total	Long	10	记录总数。

示例

请求示例

```
http(s)://[Endpoint]/?Action=DescribeOpEntities
&EndTime=1536715558000
&PageNo=1
&PageSize=10
&StartTime=1534123558000
&<公共请求参数>
```

正常返回示例

`XML` **格式**

```
<DescribeOpEntitiesResponse>
     <OpEntities>
          <element>
               <entityObject>1.1.1.1</entityObject>
               <gmtCreate>1120384</gmtCreate>
               <opAction>2</opAction>
               <opDesc>
                    <newValue>
                         <elasticBandwidth>30</elasticBandwidth>
                    </newValue>
                    <oldValue>
                         <elasticBandwidth>10</elasticBandwidth>
                    </oldValue>
               </opDesc>
               <opResult>1</opResult>
          </element>
```

```
      </OpEntities>
      <Total>10</Total>
</DescribeOpEntitiesResponse>
```

JSON 格式

```
{
 "OpEntities":[
  {
   "gmtCreate":1120384,
   "entityObject":"1.1.1.1",
   "opResult":1,
   "opDesc":{
    "newValue":{
     "elasticBandwidth":30
    },
    "oldValue":{
     "elasticBandwidth":10
    }
   },
   "opAction":2
  }
 ],
 "Total":10
}
```

错误码

访问错误中心查看更多错误码。

5.9 错误码

错误代码	描述	语义
InvalidOrderType	Invalid Order Type.	无效的订单类型。
InvalidBaseBandwidth	Invalid Base Bandwidth.	无效的基础带宽。
InvalidElasticBandwidth	Invalid Elastic Bandwidth.	无效的弹性带宽。
InvalidPortLimit	Invalid Port Limit.	无效的端口数量。
InvalidDomainLimit	Invalid Domain Limit.	无效的域名数量。
InvalidNormalBandwidth	Invalid Normal Bandwidth .	无效的业务带宽。
InvalidInstanceId	Invalid Instance Id.	无效的实例ID。
InvalidAliUid	Invalid Ali Uid.	无效的aliUid。
InstanceIdFormatError	Instance Id format error.	实例ID格式错误。
InvalidPageNo	Invalid Page No.	无效的页号。
InvalidPageSize	Invalid Page Size.	无效的分页大小。
InvalidLine	Invalid Line.	无效的合营资源。

错误代码	描述	语义
InvalidStatus	Invalid Status.	无效的状态。
InvalidExpireTime	Invalid Expire Time.	无效的过期时间。
InvalidProductType	Invalid Product Type.	无效的产品类型。
InvalidStartTime	Invalid Start Time.	无效的开始时间。
InvalidEndTime	Invalid End Time.	无效的结束时间。
InvalidInstanceIdsSize	Invalid instanceIds size.	实例ID个数超长。
InvalidInstanceRemark	Invalid instance remark.	无效的实例备注。
InternalError	Internal Error!	内部错误。
ddos_coop3000	unknown error	未知错误。
ddos_coop3001	error request method	无效的请求方式。
ddos_coop3002	http call failed	http请求调用失败。
ddos_coop3003	no authority to do request	无权请求。
ddos_coop3004	receive unknown action	无效的操作请求。
ddos_coop3005	auth failed	认证失败。
ddos_coop3006	query db failed	查询数据库失败。
ddos_coop3007	remote call selb central failed	调用中心管控服务失败。
ddos_coop3008	remote call ddos web failed	调用服务失败。
ddos_coop3101	encoding json failed	编码失败。
ddos_coop3102	decoding json failed	解码失败。
ddos_coop3103	failed parse string to int	从字符串解析数字失败。
ddos_coop3201	no enough params in request	传入的参数不足。
ddos_coop3202	params out of range	传入的参数超出允许的范围。
ddos_coop3203	start time must less then end time	开始时间必须早于结束时间。
ddos_coop3301	no instance for process in db	在数据库中未找到指定实例。
ddos_coop3302	reache port limit in spec	达到端口规格上限。
ddos_coop3303	l4 rule port is exist	转发规则已存在。

错误代码	描述	语义
ddos_coop3304	invalid rs ip address	无效的IP地址信息。
ddos_coop12001	backend service exception	服务异常。
ddos_coop12003	system exception	系统异常。
ddos_coop12010	illegal sign	无效签名。
ddos_coop12020	illegal timestamp	无效时间戳。
ddos_coop12030	illegal format	无效数据返回格式。
ddos_coop12040	illegal service	服务不存在。
ddos_coop12052	illegal aliyun idkp	aliUid参数没传或为空。
ddos_coop12302	listener not exists	指定监听不存在。
ddos_coop12610	lb or vs 或not exist	指定LB或监听不存在。
ddos_coop13000	db failed	数据库连接异常。
ddos_coop13001	failed	配置参数错误。
ddos_coop13010	json err	格式错误。
ddos_coop13020	param not enough	配置参数缺失。
ddos_coop13104	eip is released	ip已被释放。
ddos_coop13105	eip not exist	ip不存在。
ddos_coop15001	action not exist	指定操作不存在。
ddos_coop16020	auth fail	身份验证失败。
ddos_coop20403	auth failed	认证失败。
ddos_coop20404	not found	服务未发现。
ddos_coop21001	invalid parameter	无效参数。
ddos_coop21002	invalid method	无效方法。
ddos_coop21003	invalid product	无效产品。
ddos_coop21004	invalid region	无效区域。
ddos_coop21005	no action found	无此操作。
ddos_coop21006	invalid action	无效操作。
ddos_coop221007	action disabled	接口被禁用。
ddos_coop29999	system error	系统错误。

6 流量调度器

DDoS高防流量调度器允许您设置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，保证无DDoS攻击时日常业务的流畅体验以及发生DDoS攻击时更好的防护效果。流量调度器提供云产品联动、阶梯防护、CDN联动功能。本文介绍了它们的使用场景和配置方法。

使用场景

下表描述了DDoS高防流量调度器的不同功能的使用场景。

功能	使用场景	使用效果
云产品联动	日常不使用高防，无延迟增加；被攻击时，需要将DDoS高防前置，防护DDoS攻击。	无攻击时，高防做备用，不增加延迟；被攻击时，切换至DDoS高防。 
阶梯防护	日常使用防护包防御DDoS，无延迟增加；被大流量攻击的时候，需要切到DDoS高防。	防护包抵御日常攻击，不增加延迟；大流量攻击时，切换至DDoS高防。 
CDN联动	网站使用CDN加速，又需要防御DDoS攻击；当攻击发生时，需要从CDN切换至DDoS高防。	无攻击时，就近使用CDN节点加速；被攻击时，切换至DDoS高防。 

使用限制

下表描述了DDoS高防流量调度器的不同功能的使用限制。

功能	限制条件	说明
云产品联动	高防实例规格	DDoS高防实例的QPS、业务带宽等规格满足正常业务防护需求，当流量切至高防时，确保可以承载业务流量。
	高防配置	DDoS高防实例预先完成被防护业务的转发配置。
阶梯防护	防护包	购买并使用防护包企业版。
	实例规格	防护包业务带宽规格满足防护需求。
	高防配置	DDoS高防实例预先完成被防护业务的转发配置。
	防护包配置	云资源在防护包的防护对象中。

功能	限制条件	说明
CDN联动	CDN状态	域名不允许是切入沙箱状态。  说明: 如果域名已经被CDN切入沙箱，建议您只用DDoS高防，不用联动。
	攻击频率	不适合被攻击频率太高的网站，例如高于每周3次以上。
	防护生效敏感度	不适合对防护生效速度要求比较高的场景。  说明: 调度到DDoS高防时，防护生效时间受DNS TTL生效时间限制。
	业务流量	不适合正常业务流量和QPS比较大的场景。  说明: 若超过3 Gbps、10000 QPS时，请提交工单进行评估。
	业务类型	只适合HTTP和HTTPS业务，不支持视频直播。
	高防版本	仅支持增强功能版本的DDoS高防实例。

启用CDN联动功能时，您需要设置访问QPS阈值，作为CDN和DDoS高防间相互切换的条件。CDN和DDoS高防间相互切换满足以下逻辑和限制。

- CDN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，则触发切换流程。
  - CDN上流量不超过10 Gbps。

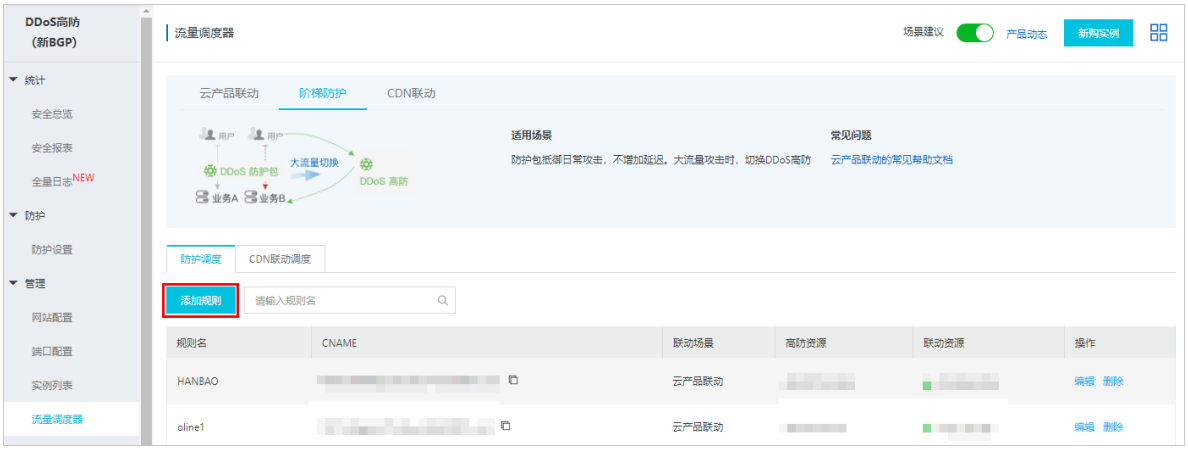
     说明:
    10 Gbps超出了DDoS高防的售卖规格。
- 高防切换到CDN
  - 连续12小时以上，域名QPS低于QPS阈值的80%、CC阻断率低于10%，则触发回切流程。
  - 回切检查：要切回的高防IP不在清洗黑洞中且1小时内不存在清洗、黑洞事件。
  - 回切时间范围：上午8时到晚上23时，其他时间不触发回切。

配置概述

功能	配置说明
云产品联动	云产品联动分为云产品与DDoS高防一对一切换、云产品与DDoS高防多对一切换。 配置步骤如下。 1. 配置DDoS高防转发。参见添加网站配置。 2. 验证高防实例可以正常转发。参见验证配置生效。 3. 配置流量调度器。 · 一对一切换，参见添加防护调度规则。 · 多对一切换，包括以下两种配置模式： - 优先使用云产品，无可用云产品IP时，切换高防。配置方法同一对一切换，在添加防护调度规则时，选择添加多个需要联动的云资源IP即可。 - 云产品多路分摊流量，每路被攻击单独切换高防。配置方法参见多路分摊切换配置示例。 4. 将DNS解析到流量调度器。修改域名的DNS解析，应用CNAME解析并将解析目标设置为调度器分配的CNAME地址。 说明: 关于修改域名DNS解析CNAME记录的操作步骤，业务接入DDoS高防配置可供参考，但请注意应该应用流量调度器分配的CNAME地址，而不是DDoS高防CNAME地址。
阶梯防护	阶梯防护分为防护包中云产品与DDoS高防一对一切换、防护包中云产品与DDoS高防多对一切换。配置步骤与云产品联动相同。
CDN联动	配置步骤如下。 1. 预先配置好CDN，并解析到CDN，经测试可用。 参见添加加速域名。 说明: 如果配置了源站防护（安全组），则需要将CDN回源地址加白。 2. 配置DDoS高防转发。参见添加网站配置。 3. 验证高防实例可以正常转发。参见验证配置生效。 4. 配置流量调度器。参见添加CDN联动。 5. 将DNS解析到流量调度器。修改域名的DNS解析，应用CNAME解析并将解析目标设置为调度器分配的CNAME地址。 说明: 关于修改域名DNS解析CNAME记录的操作步骤，业务接入DDoS高防配置可供参考，但请注意应该应用流量调度器分配的CNAME地址，而不是DDoS高防CNAME地址。

添加防护调度规则

1. 登录云盾DDoS高防控制台。
2. 在左侧导航栏，单击管理 > 流量调度器。
3. 在防护调度页签下，单击添加规则。

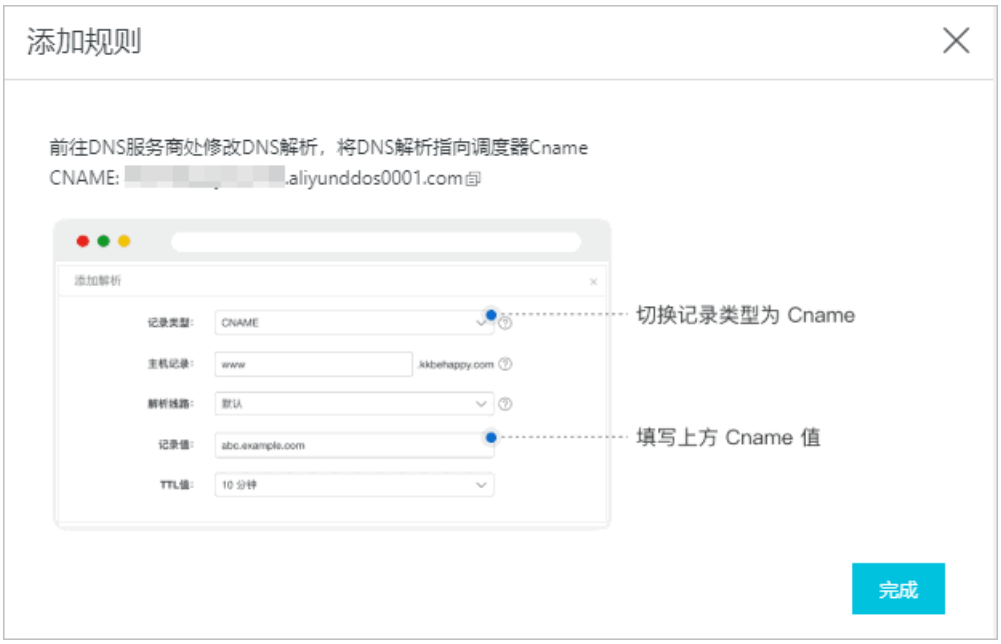


4. 在添加规则侧边页，完成联动规则配置，并单击下一步。联动规则的配置描述见下表。

配置项	说明
联动场景	选择规则类型，取值： · 云产品联动 · 阶梯防护 说明： 仅支持DDoS防护包防护对象中的云资源，包括ECS、EIP、SLB、WAF。
规则名	为规则命名。规则名由英文字母、数字和下横线（_）组成，且不超过128个字符。
高防IP	选择要联动的高防实例。

配置项	说明
云资源	设置要联动的云资源。选择云资源所在地域，并输入云资源IP地址。单击添加源资源IP，可以添加多个云资源。最多支持添加20个IP。

成功添加规则，调度器为新建规则分配一个CNAME地址。要使调度规则生效，您需要前往云资源的DNS服务商处修改其DNS解析，应用CNAME解析并将解析目标设置为调度器分配的CNAME地址。



您可以在防护调度规则列表中查看新建的规则和CNAME地址。

添加CDN联动

1. 登录云盾DDoS高防控制台。
2. 在左侧导航栏，单击管理 > 流量调度器。
3. 打开CDN联动调度页签。

   CDN联动调度页签展示了所有已添加到DDoS防护中的网站域名。
4. 定位到要配置的域名，单击其操作列下的添加联动。

5. 在添加联动侧边页，确认域名信息满足要求后，配置切换至高防条件，即访问QPS的最小值，并单击下一步。

   要添加联动，域名信息应满足以下要求。

   - 高防资源：已开通增强功能。

   - 联动资源：已完成阿里云CDN配置。

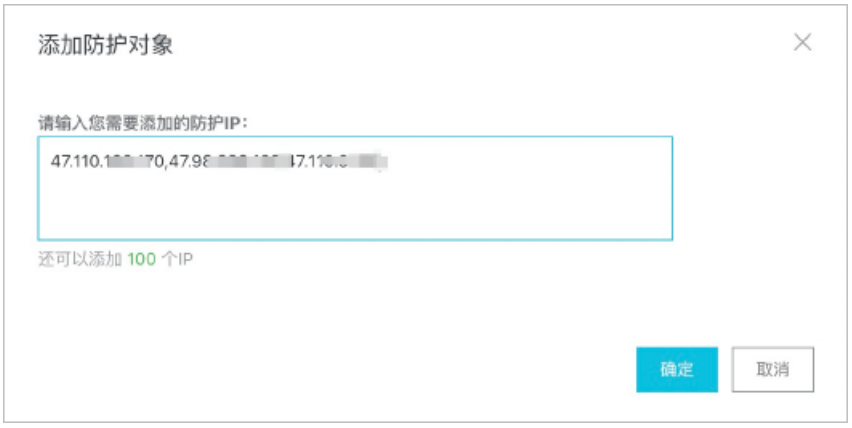
   成功添加联动，调度器为新建规则分配一个CNAME地址。要使调度规则生效，您需要前往云资源的DNS服务商处修改其DNS解析，应用CNAME解析并将解析目标设置为调度器分配的CNAME地址。

您可以在CDN联动调度规则列表中看到域名的CDN联动状态更新为已开启，并查看其CNAME地址。

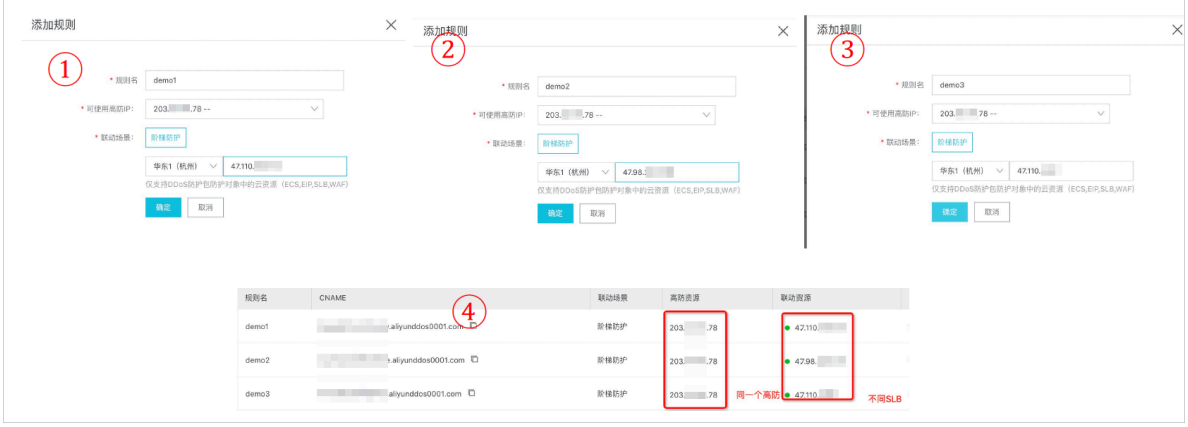
多路分摊切换配置示例

以多防护包切换DDoS高防为例，介绍云产品与DDoS高防多对一切换（云产品多路分摊流量，每路被攻击单独切换高防模式）的具体配置方法。其中，CNAME解析记录的更新以阿里云云解析DNS为例截图说明。

1. 防护包配置。在防护包中添加多个防护对象，示例中是三个。



2. 流量调度器配置。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高防IP。



3. 域名解析配置。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。

4. 验证结果。在*http://tool.chinaz.com/*上验证步骤3中添加的CNAME记录生效。

7 安全专家指导服务

阿里云新BGP高防IP产品为您免费提供一对一的专家指导咨询服务。

背景信息

如果您在使用云盾新BGP高防IP产品过程中遇到任何问题，可以随时通过云盾新BGP高防IP管理控制台的专家咨询服务入口，申请加入阿里云企业安全服务钉钉群。

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

操作步骤

1. 登录云盾新BGP高防IP管理控制台。
2. 将鼠标移至有问题？找专家！图标，使用钉钉扫描显示的二维码申请加入阿里云企业安全服务钉钉群。

说明:

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

3. 成功加入阿里云企业安全服务钉钉群后，安全专家将通过钉钉为您提供一对一指导服务，帮助您妥善解决新BGP高防IP产品使用过程中遇到的任何问题。

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