阿里云
DDoS高防IP

DDoS高防（国际）

文档版本：20200131

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DDoS高防（国际）

针对用户业务服务器部署在中国大陆以外地域的场景，阿里云提供云盾DDoS高防（国际）付费增值服务，帮助您缓解DDoS攻击风险。

通过为您部署在海外地区的服务器配置DDoS高防（国际）服务，将您服务器遭受的攻击流量牵引至DDoS高防（国际）的独享IP，通过全球级分布式近源清洗的方式清洗攻击流量，并将过滤后的正常流量返回至源站服务器，从而保障您的业务稳定运行。

相关文档

- **网站业务接入DDoS高防（国际）防护**
- **非网站业务接入DDoS高防（国际）防护**
- **配置DDoS高防（国际）加速线路**

1.2 功能特性

DDoS高防（国际）为您提供以下DDoS攻击防御功能。

功能项	描述
过滤畸形报文	过滤Frag flood，Smurf、stream flood、Land flood攻击，过滤IP畸形包、TCP畸形包、UDP畸形包等畸形报文。
防御传输层DDoS攻击	过滤Syn flood、Ack flood、UDP flood、ICMP flood、Rst flood等攻击。
防御Web应用DDoS攻击	过滤HTTP Get flood、HTTP Post flood、高频攻击。同时，支持根据HTTP特征、URI、Host进行过滤。

产品特性

DDoS高防（国际）服务具有以下特性：

- **全球近源清洗**

  通过Anycast通信模式充分利用全球各地阿里云流量清洗中心的能力作为DDoS高防（国际）服务的资源，采用分布式技术将DDoS攻击流量自动牵引至距离攻击源最近的流量清洗中心进行过滤，在将防护能力进行整合实现最大化的同时也具备多机房备份容灾的能力。

- 无上限全力防护

  与中国大陆地区的DDoS高防IP服务不同，DDoS高防（国际）服务依托全球近源清洗能力，为每位用户提供不设上限的全力防护。

  2018年，阿里云海外地区高防流量清洗中心的总能力将超过2Tbps。DDoS高防（国际）服务以为您成功防御每一次DDoS攻击为目标，充分运用全球阿里云流量清洗中心的防护能力为您的业务提供最大限度的防护，在您的业务发展过程中为您保驾护航。

  > 注意:
  > 如果您业务遭受的攻击影响到阿里云海外高防清洗中心基础设施时，阿里云保留压制流量的权利。一旦对您的DDoS高防（国际）进行流量压制，可能对您的业务造成一定影响，例如您的业务访问流量可能会被限速，甚至被黑洞。

- 独享IP资源

  DDoS高防（国际）服务为每位用户提供一个独享Anycast IP，各IP之间互相隔离，避免其它用户遭受的DDoS攻击对您的业务产生任何误伤，为您提供更加安全的DDoS防护服务。

- 安全防护报表

  DDoS高防（国际）服务为您实时提供详细的流量报表及攻击防护详细信息，让您及时、准确地了解当前业务的安全状态。

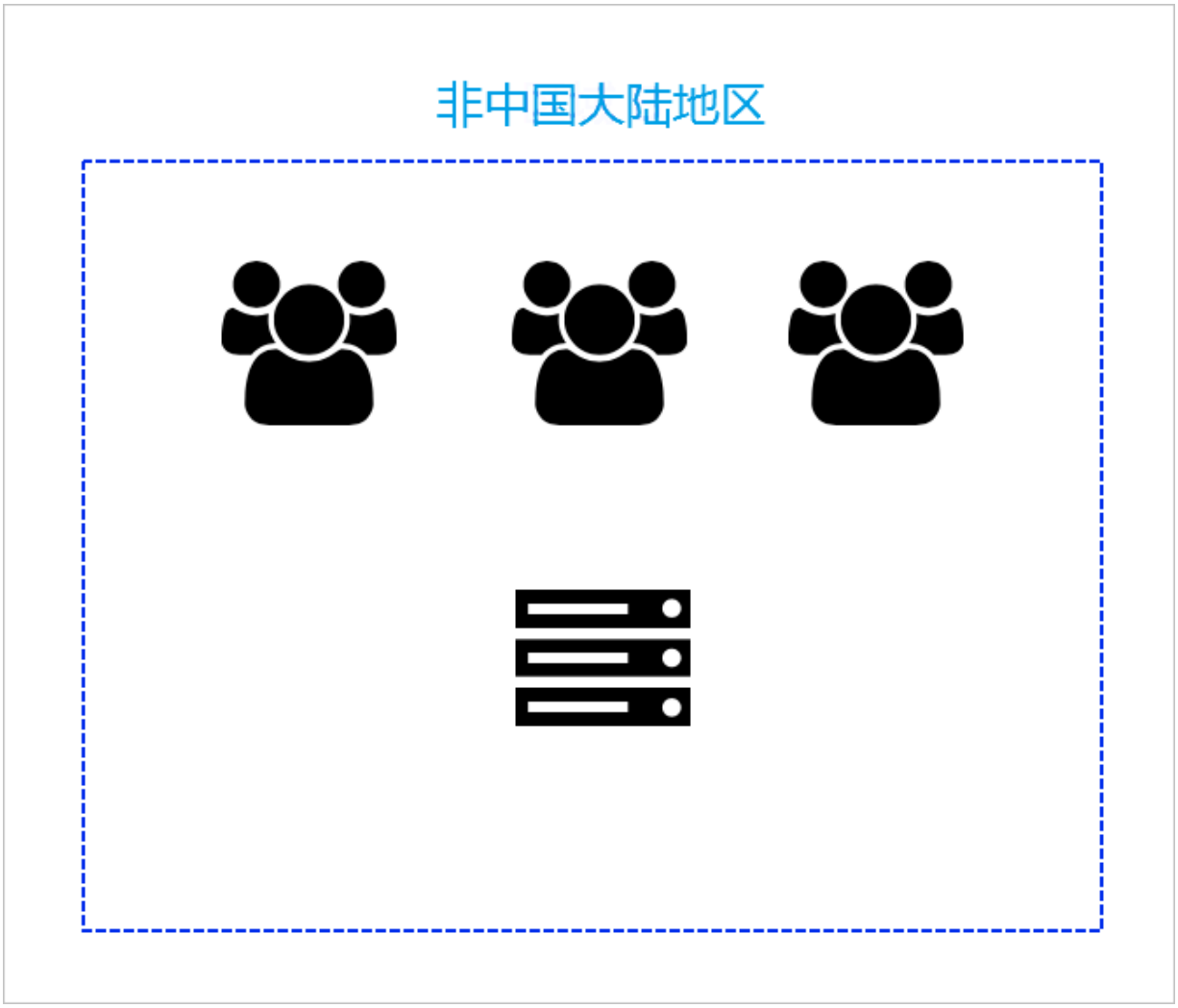
1.3 DDoS高防（国际）应用场景

DDoS高防（国际）的主要应用场景：互联网Internet通过各地网络运营商互联来实现全球范围内的互通访问，但由于各个区域的网络运营商的策略不同，导致网络访问互通的实际情况各不相同，因此您需要根据不同的业务场景选择最合适的DDoS安全防护解决方案。

> 说明:
> 基于当前网络运营商的路由互联策略，默认情况下从中国大陆地区访问海外DDoS高防资源，单独使用DDoS高防（国际）服务无法保证该场景的网络链路质量。
>
> 此场景存在的问题包括：访问延迟平均高达300ms，并且可能受国际链路拥塞影响而导致间歇性丢包。因此，强烈建议您在中国大陆地区部署服务器来服务中国大陆用户，同时使用中国大陆地区的DDoS高防服务解决DDoS安全防护问题，并且遵守相关中国法律法规完成网站备案等合规手续。

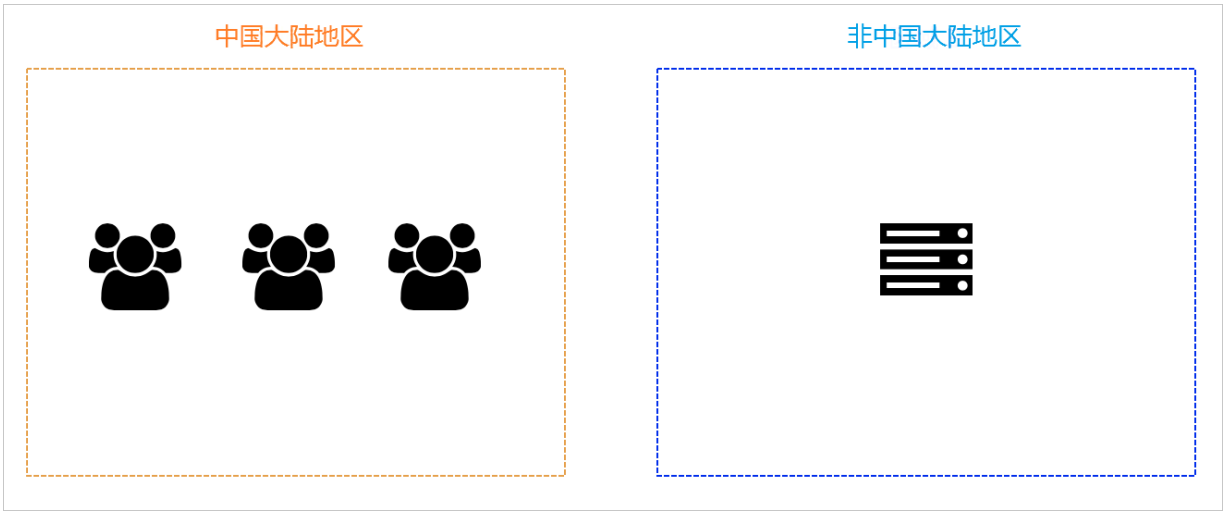
对于服务器部署在非中国大陆地区的业务，主要可分为以下三个场景：

场景一：业务服务器部署在非中国大陆地区，且主要服务于非中国大陆地区的用户



推荐方案：购买DDoS高防（国际）服务，根据*DDoS高防（国际）快速入门*将业务接入高防进行防护。

场景二： 业务服务器部署在非中国大陆地区，主要服务于中国大陆地区的用户



推荐方案：

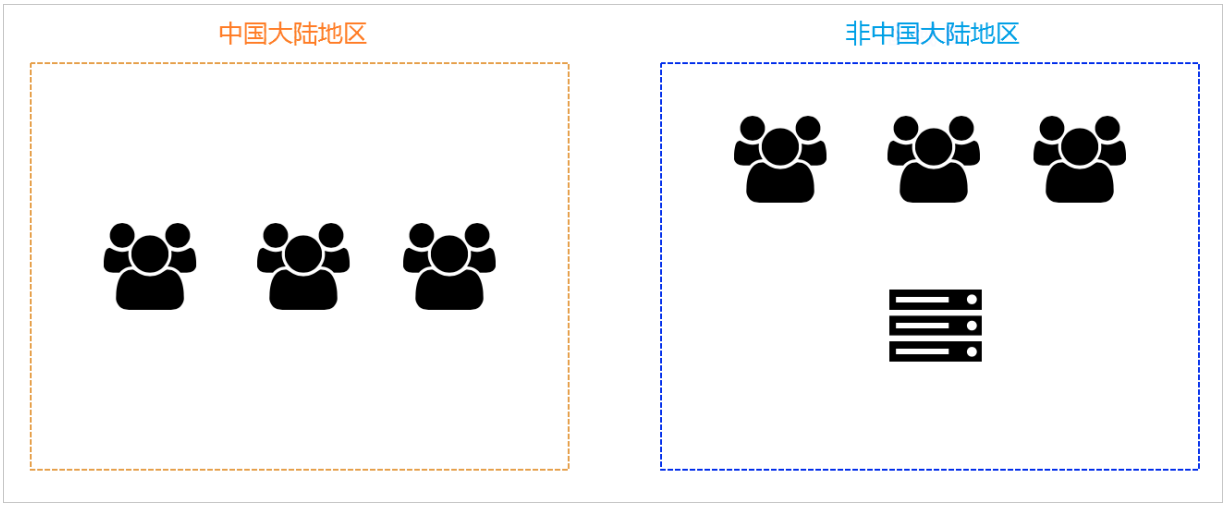
- **方案一**

  如果您的业务对网络延迟要求比较高（例如游戏业务服务器），建议您将服务器迁移至您的主要用户所在的中国大陆地区，并且购买*DDoS*高防*IP*服务或新*BGP*高防*IP*服务来缓解DDoS攻击。

- **方案二**

  如果您的业务服务器暂时无法迁移到中国大陆地区，联系销售或通过工单申请购买开通DDoS高防（国际）加速线路。开通后，阿里云技术支持人员将协助您完成DDoS高防智能切换方案配置，实现在无DDoS攻击时通过加速线路保障中国大陆地区用户访问顺畅的需求。关于DDoS高防（国际）加速线路配置，参考配置*DDoS*高防（国际）加速线路。

场景三： 业务服务器部署在非中国大陆地区，同时服务中国大陆和非中国大陆地区的用户



推荐方案：

- **方案一**

  建议您分区域部署业务服务器，用部署在中国大陆地区的服务器服务中国大陆地区用户，部署在非中国大陆地区的服务器服务非中国大陆地区用户。同时，通过购买*DDoS*高防*IP*服务或新*BGP*高防*IP*服务和DDoS高防（国际）服务分别保护中国大陆地区和非中国大陆地区的业务，缓解DDoS攻击。

- **方案二**

  如果您暂时无法在中国大陆地区部署业务服务器，联系销售或通过工单申请购买开通DDoS高防（国际）加速线路。开通后，阿里云技术支持人员将协助您完成DDoS高防智能切换方案配置，实现在无DDoS攻击时通过加速线路保障中国大陆地区用户访问顺畅的需求。关于DDoS高防（国际）加速线路配置，参考配置*DDoS*高防（国际）加速线路。

2 产品定价

2.1 计费方式

DDoS高防（国际）服务提供保险版和无忧版两种套餐版本供您选择。

DDoS高防（国际）的高级防护

DDoS高防（国际）的高级防护是以成功防护每一次DDoS攻击为目标，整合阿里云海外地区所有高防清洗中心能力全力保护用户业务。

大部分情况显示，持续使用DDoS高防服务并成功防护攻击的用户遭受攻击的风险将明显下降。一般来说，恶意攻击者发起攻击背后的目的是为了对目标业务造成损失。由于发起攻击本身也存在成本，如果攻击始终无法达到目的，攻击便会停止。因此，DDoS高防（国际）的高级防护不设防护上限，调用阿里云海外地区所有高防清洗中心能力，全力保障用户业务。

注意:
如果您业务遭受的攻击影响到阿里云海外高防清洗中心基础设施时，阿里云保留压制流量的权利。一旦对您的DDoS高防（国际）进行流量压制，可能对您的业务造成一定影响，例如您的业务访问流量可能会被限速，甚至被黑洞。

DDoS高防（国际）的套餐版本

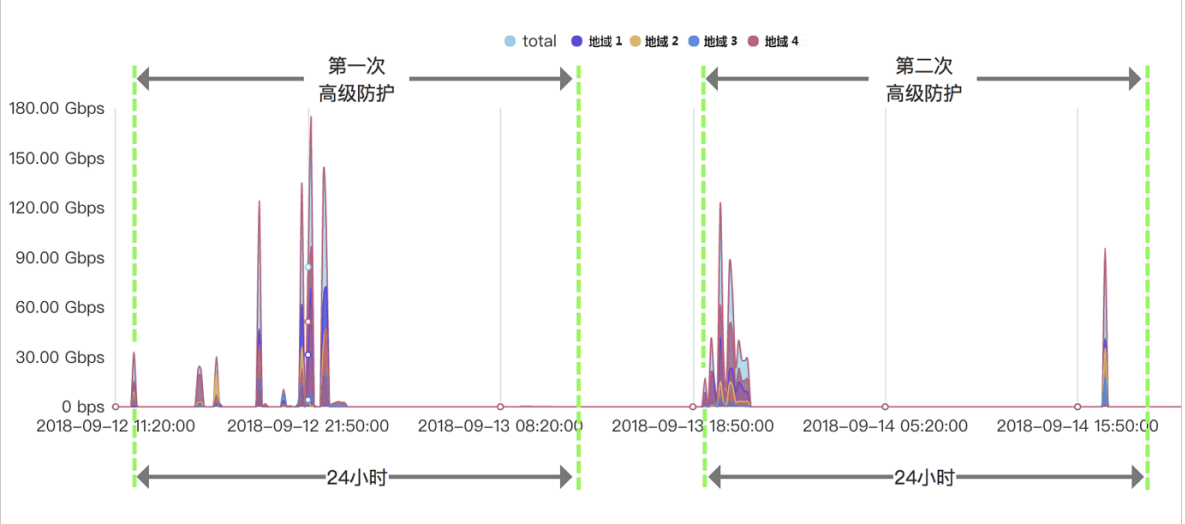
- **保险版**

  DDoS高防（国际）保险版包含每月两次高级防护（无上限全力防护），自遭受流量攻击起24小时内为您的业务提供无上限全力防护，并消耗一次高级防护使用次数。每月初您的DDoS高防（国际）实例的高级防护使用次数将自动重置为两次。

  说明:
  如果您需要更多高级防护次数，可额外购买全局高级防护。

  例如，自9月12日11:20:00起所防护的IP遭到流量攻击，触发高级防护，24小时内DDoS高防（国际）为该业务提供无上限全力防护。9月13日18:50:00该业务再次遭受流量攻击并触发

高级防护，24小时后无上限全力防护结束，且9月两次高级防护使用次数消耗完毕。DDoS高防（国际）保险版实例的高级防护使用次数将在下月初（10月1日）自动重置。



保险版作为DDoS高防（国际）的入门方案，适用于受攻击风险较低的用户。

- 无忧版

  DDoS高防（国际）无忧版为您提供无限次高级防护（无上限全力防护）。选购无忧版套餐，您无需担心攻击大小和攻击次数，DDoS高防（国际）服务将全面为您的业务保驾护航。

DDoS高防（国际）的产品定价

DDoS高防（国际）实例的具体定价如下表所示：

套餐类型	业务带宽	高级防护	单价（元/月）
保险版	100 Mbps	2 次/月	17,500
无忧版		无限次	77,000
保险版	150 Mbps	2 次/月	22,750
无忧版		无限次	84,000
保险版	200 Mbps	2 次/月	28,000
无忧版		无限次	91,000
保险版	250 Mbps	2 次/月	33,250
无忧版		无限次	98,000
保险版	300 Mbps	2 次/月	37,100
无忧版		无限次	105,000

说明:

如果您需要更高的业务带宽规格，请联系阿里云技术支持人员。

> **说明:**
> 业务带宽指无攻击情况下DDoS高防（国际）实例支持处理的最大正常业务带宽。请确保实例的业务带宽大于所需接入实例防护的所有业务的网络入、出方向总流量峰值中较大的值。关于业务带宽的详细说明，查看如何选择业务带宽。
>
> 超出最大业务带宽后，将出现限流、随机丢包等现象，可能导致您的正常业务在一定时间内出现不可用、卡顿、延迟等问题。

同时，DDoS高防（国际）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。	5个	每5个端口： 1,000元/月
防护域名数	实例支持添加的HTTP/HTTPS域名数量。	10个 **说明:** 最多涉及一个一级域名。即所添加的域名所属的一级域名总数不超过1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。	· 保险版：500 QPS · 无忧版： 1,000 QPS	每100 QPS： 1,000元/月

到期说明

- 服务距离到期时间前的29、27、3、1天，会通过短信/邮件的形式提醒您服务即将到期，并提醒您续费。
- 如到期后没有续费，DDoS防护会恢复到默认的免费防护能力。

- 服务到期后您的 DDoS高防（国际）相关配置为您保留一个月（30天）。一个月内完成续费，则可继续使用原DDoS高防（国际）实例；一个月后，DDoS高防（国际）实例自动释放，服务将不可用。

不支持退款声明

阿里云DDoS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DDoS高防实例，一概不支持退款。

更多信息

选择业务带宽规格

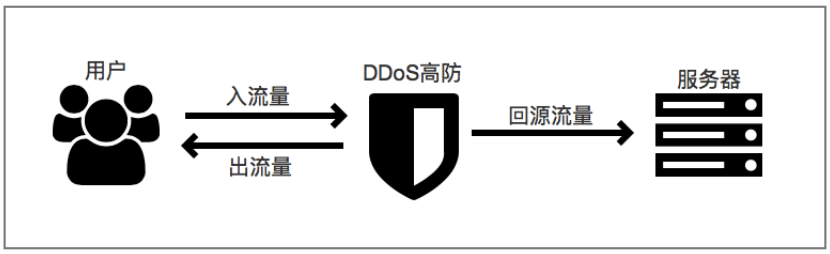
您可以根据所有已经或将要接入DDoS高防（国际）实例的业务的日常入方向或出方向总流量的峰值，选择合适的业务带宽规格。您选择的最大业务带宽应大于这些业务的网络入、出方向总流量峰值中较大的值。

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DDoS高防（国际）进行防护。在业务正常访问（未遭受攻击）时，DDoS高防（国际）将这些正常访问流量回源到源站服务器；而当业务遭受攻击时，DDoS高防（国际）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DDoS高防（国际）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DDoS高防（国际）实例默认支持添加10条域名配置记录，且仅支持接入1个一级域名。

例如，默认情况下，您可以添加一个一级域名（例如`abc.com`），且为该域名本身和它的子域名或泛域名（例如，`www.abc.com`，`*.abc.com`，`mail.abc.com`，`user.pay.abc.com`，`x.y.z.abc.com`等）添加10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。

如果您想要添加两个不同的一级域名或它们的子域名接入该DDoS高防（国际）实例进行防护，您需要扩展防护域名数规格。假设您已经添加`abc.com`或其子域名进行防护，当您尝试添加`xyz.com`（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DDoS高防（国际）实例额外增加10个防护域名数量。

2.2 全局高级防护次数

如果已购买的DDoS高防（国际）保险版实例当月提供的两次高级防护次数已耗尽，您可以额外购买全局高级防护次数获得更多高级防护（无上限全力防护）使用次数。

DDoS高防（国际）保险版实例默认包含每月两次的高级防护（无上限全力防护），自遭受流量攻击起24小时内为您的业务提供无上限全力防护，并消耗一次高级防护使用次数。

如果所防护的业务遭受频繁的大流量攻击，保险版实例默认的两次高级防护可能无法完全保证业务的可用性，您可以购买全局高级防护补充您账号中所有DDoS高防（国际）保险版实例的高级防护使用次数。

使用说明

当您的保险版实例当月默认的两次高级防护次数耗尽后，如果所防护的业务再次遭受大流量攻击且攻击流量超过基础防护阈值时，将消耗您所购买的全局高级防护次数为业务提供高级防护（无上限全力防护）。

全局高级防护次数无需绑定实例，可供您账号中所有符合使用条件的保险版实例使用。

使用条件

- **保险版实例在有效期内。**

- 账号的高级防护功能未冻结。

> **说明：**
> 当您账号中所有实例当月消耗的高级防护次数（包含当月已消耗的全局高级防护次数）已经超过10次，高级防护功能将自动被冻结，需要等到下个自然月方能恢复使用。
>
> 如果您的业务确实频繁遭受大流量攻击，建议您选购无忧版实例进行防护。

购买全局高级防护次数

您购买DDoS高防（国际）实例后，随时可以在DDoS高防（国际）管理控制台中购买全局高级防护次数。

1. 登录*DDoS高防（国际）管理控制台*。
2. 在实例列表页面，单击右上方的购买。

3. 在全局高级防护购买页面中，选择需要购买的次数，单击立即购买。

> **说明：**
> 购买时请确认所选择的适用产品是DDoS高防（国际）。

产品定价

定价参数	说明
付费方式	预付费
有效时长	1年
购买单价	10,500 元/次

> **注意：**
> 全局高级防护次数不支持退款。

更多信息

全局高级防护与DDoS高防（国际）实例高级防护

类型	所属范围	有效期	使用次数
无忧版实例高级防护	实例	根据实例有效期	无限次
保险版实例高级防护	实例	一个月 说明: 当月未消耗的高级防护次数在下月初将被清空。	两次/月
全局高级防护	云账号	一年	单独购买

2.3 加速线路

如果您的业务服务器部署在非中国大陆地区，可以为您的DDoS高防（国际）实例加购加速线路，实现中国大陆地区用户对您的业务的访问加速。

加速线路用于降低中国大陆地区用户对您部署在非中国大陆地区业务的访问延迟，大幅提升在无攻击情况下的访问质量。

说明:
加速线路不支持单独配置使用。加速线路实例本身不具备任何防护能力，因此必须与DDoS高防（国际）保险版或无忧版实例搭配使用。

关于加速线路的推荐应用场景，查看*DDoS*高防（国际）应用场景。

购买加速线路实例后，您可按照配置*DDoS*高防（国际）加速线路将加速线路与已购买的DDoS高防（国际）保险版或无忧版实例搭配使用，实现无攻击状态下业务针对中国大陆地区用户的加速访问。

产品定价

DDoS高防（国际）加速线路的具体定价如下表所示：

业务带宽	单价（元/月）
10 Mbps	10,000
20 Mbps	20,000
30 Mbps	30,000
40 Mbps	40,000
50 Mbps	50,000
60 Mbps	60,000

业务带宽	单价（元/月）
70 Mbps	70,000
80 Mbps	80,000
90 Mbps	90,000
100 Mbps	100,000

说明:

业务带宽指无攻击情况下DDoS高防（国际）加速线路实例支持处理的最大正常业务带宽。请确保实例的业务带宽大于所需接入加速线路实例的所有业务的网络入、出方向总流量峰值中较大的值。

超出最大业务带宽后，将出现限流、随机丢包等现象，可能导致您的正常业务在一定时间内出现不可用、卡顿、延迟等问题。

到期说明

- **服务距离到期时间前的29、27、3、1天，会通过短信/邮件的形式提醒您服务即将到期，并提醒您续费。**
- **如到期后没有续费，加速线路实例将停止提供访问加速能力。**
- **服务到期后您的加速线路实例相关配置为您保留一个月。一个月内完成续费，则可继续使用原加速线路实例；一个月后，加速线路实例自动释放，服务将不可用。**

2.4 功能套餐说明

DDoS高防（国际）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DDoS高防（国际）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DDoS高防（国际）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，您可以通过实例升级开通增强功能。

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DDoS高防（国际）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*启用AI智能防护*。	✓	✓
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。	✓	✓

功能分类	功能项	功能描述	标准功能套餐	增强功能套餐
	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。	✗	✓
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。	✗	✓

3 快速入门

3.1 接入DDoS高防（国际）

DDoS高防（国际）服务支持您将网站域名（七层）或业务端口（四层）配置接入实现对您业务的DDoS攻击防护。

购买DDoS高防（国际）实例后，您可以在控制台中为您的网站域名或业务端口添加接入配置信息，并配置转发规则指定流量清洗后正常流量所需回送到源站服务器。

在控制台中完成上述配置后，您将DNS域名解析或直接将业务IP指向DDoS高防（国际）服务分配的IP或CNAME的方式，将流量切换至DDoS高防（国际）实例。实现所有业务访问流量先经过DDoS高防（国际）实例，再由DDoS高防（国际）实例转发至源站服务器的业务模式，您的业务即可享受由DDoS高防（国际）服务为您提供的无上限全力DDoS攻击防护。

3.2 网站业务接入DDoS高防（国际）防护

购买DDoS高防（国际）实例后，您可以将您的网站业务接入DDoS高防（国际）实例，实现DDoS攻击防护。如果您需要将端游、手游、APP等非网站业务接入DDoS高防（国际）实例进行防护，请参见非网站业务接入DDoS高防（国际）。

操作步骤

1. 登录*DDoS*高防（国际）管理控制台。
2. 在左侧导航栏，单击接入配置。
3. 在网站接入页签下，单击添加网站。
4. 在填写网站信息任务中，添加要防护的网站信息，并单击添加。配置描述见下表。

配置项	说明
功能套餐	选择功能套餐规格。取值： · 标准功能 · 增强功能

配置项	说明
实例	为要接入的网站域名关联DDoS高防（国际）实例。一个网站域名最多支持关联8个DDoS高防（国际）实例，且不支持关联不同功能套餐的实例。 根据您在功能套餐中选择的功能套餐类型显示对应的DDoS高防（国际）实例供您选择。如果无可选实例，表示您当前无可用的该功能套餐规格的DDoS高防（国际）实例。您可以选择新购实例或升级已有的标准功能套餐实例。
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`。DDoS高防（国际）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`），DDoS高防（国际）优先使用精确域名所配置的转发规则和防护策略。
转发协议	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他协议类型。
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源站IP和源站域名。 · 源站IP：支持配置最多20个源站IP地址。配置多个源站IP后，DDoS高防（国际）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DDoS高防（国际）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	说明
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。 

配置项	说明
CnameReuse	申请开放CNAME复用功能后，选择是否启用CNAME复用。更多信息，请参见 *CNAME*复用。

成功添加网站配置。DDoS高防（国际）为每个网站配置分配一个CNAME地址，用于将网站通过CNAME接入到高防，从而将网站访问请求转发到DDoS高防（国际）实例进行防护。

单击去网站列表，您可以在网站接入列表中看到新添加的网站配置和其CNAME地址。

5. **在网站的域名解析服务提供商处，修改网站域名的DNS解析记录。为域名应用CNAME解析，并将CNAME记录值设置为DDoS高防（国际）CNAME地址，将网站业务流量切换至DDoS高防（国际）实例。**

说明:

建议您在正式切换业务流量前，在本地测试已配置的DDoS高防（国际）的转发规则已生效。在本地测试通过后，再修改DNS解析将网站业务流量切换至DDoS高防（国际）实例。

a) 登录*DDoS*高防（国际）管理控制台。

b) 在左侧导航栏，单击接入配置。

c) 在网站接入页签下，定位到已添加的域名，记录其CNAME地址。

d) 前往网站域名的DNS服务提供商处，修改DNS解析，将该网站域名解析的CNAME记录指向DDoS高防（国际）CNAME地址。

各DNS服务提供商CNAME记录的设置页面不同，请以实际页面为准，下图举例的添加CNAME记录页面仅供参考。

e) 等待DNS解析配置生效，您的网站业务流量即切换至DDoS高防（国际）实例进行防护。

说明：

一般DNS解析配置更新后大约需要十分钟左右生效，建议您在业务低峰期修改网站域名的DNS解析。

6. （可选）配置源站保护，具体操作参见高防源站保护。

说明：

配置源站保护，并不能完全防止没有经过DDoS高防（国际）实例的流量对源站直接发起DDoS攻击（甚至将源站打进黑洞）。配置高防源站保护仅对于小流量CC攻击以及Web攻击有防护意义，对于防护大规模DDoS攻击的意义并不大。

3.3 非网站业务接入DDoS高防（国际）防护

购买DDoS高防（国际）实例后，您可以将您的非网站业务（如端游、手游、APP等）接入DDoS高防（国际）实例实现DDoS攻击防护。

背景信息

注意：

- **与网站业务不同，接入非网站业务配置后只进行四层转发。DDoS高防（国际）将不会解析七层报文的内容，也不无法提供基于七层报文的防护（如CC攻击、Web攻击等），仅支持四层防护（如SYN Flood、UDP Flood等攻击防护）。**
- **为了防止私自搭建DNS防护服务器，DDoS高防国际不支持添加纯网络四层53端口的配置接入。**

说明：

如果您需要将网站业务接入DDoS高防（国际）实例进行防护，参考网站业务接入*DDoS*高防（国际）防护。

操作步骤

1. **登录*DDoS*高防（国际）管理控制台。**
2. **定位到接入配置 > 非网站接入页面，在左上侧的下拉菜单中选择DDoS高防（国际）实例，单击添加规则。**

3. 在添加规则页面，配置转发规则，单击确定。

参数	描述	说明
转发协议	该业务所需转发的协议。	支持选择TCP或UDP协议。
服务端口	DDoS高防（国际）实例对外提供服务的端口号，一般建议设置与源站相同的业务端口号。	支持设置1-65535范围任意端口号。
源站端口	源站提供业务服务的真实端口号。	支持设置1-65535范围任意端口号。
源站IP	源站服务器IP地址。	最多支持配置20个源站IP。如果配置多个回源IP，系统将自动以轮询模式将访问流量转发至源站，实现负载均衡。

4. 通过本地测试验证所配置的DDoS高防（国际）转发规则生效后，即可将业务直接指向所选择的DDoS高防（国际）实例的独享IP即可。

说明:

您可以登录*DDoS*高防（国际）管理控制台，在实例列表页面，查看DDoS高防（国际）实例所对应的独享IP。

- 如果您的业务直接通过IP进行访问，直接将业务IP替换为DDoS高防（国际）实例的独享IP。
- 如果您的业务中同时使用域名来指定服务器地址（例如，游戏客户端中设置“aliyundemo.com”域名作为服务器地址，或该域名已经写在客户端程序中），在域名的DNS解析服务提供商处修改DNS解析，将该域名的A记录指向DDoS高防（国际）实例的独享IP。

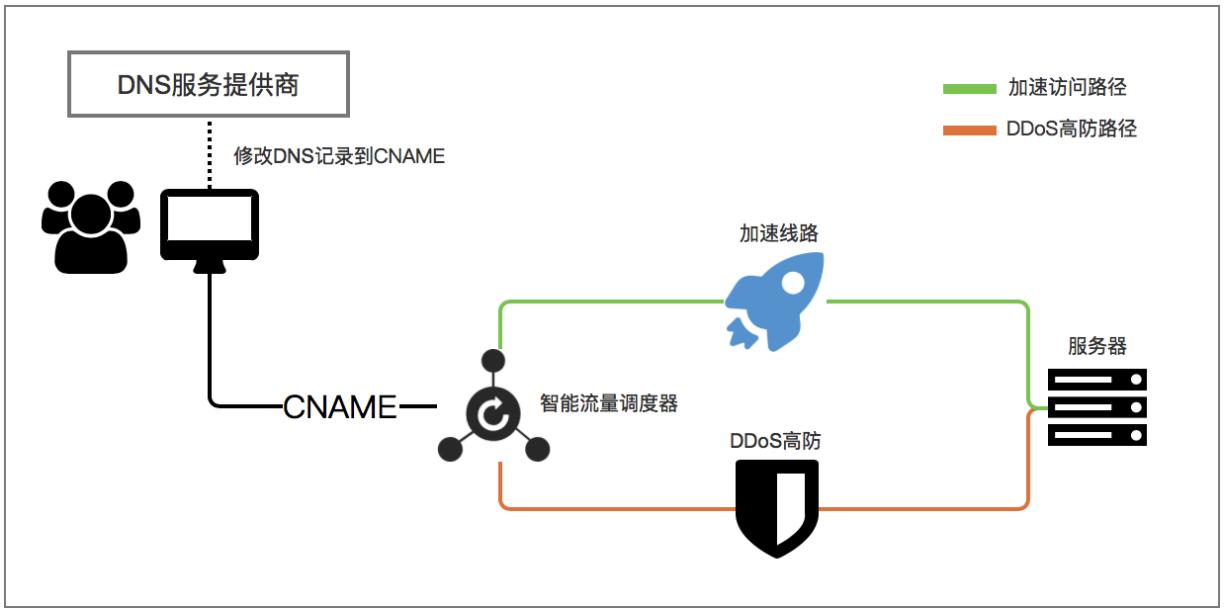
3.4 配置DDoS高防（国际）加速线路

DDoS高防（国际）加速线路需要与DDoS高防（国际）保险版或无忧版结合使用，用于实现中国大陆地区用户对您部署在非中国大陆地区业务的快速访问。

背景信息

为DDoS高防（国际）保险版或无忧版配置加速线路，可以实现当您的业务在无攻击的情况下，通过加速线路实现业务的快速访问，而当遭受攻击时自动切换至DDoS高防（国际）线路缓解DDoS攻击。

关于建议配置加速线路的场景说明，请参见*DDoS*高防（国际）应用场景。



您可以为网站域名（七层）或业务端口（四层）配置DDoS高防（国际）加速线路。

购买DDoS高防（国际）加速线路和保险版/无忧版套餐后，在DDoS高防（国际）管理控制台中将您的网站域名或业务端口配置接入DDoS高防（国际）实例进行防护，配置智能流量调度器实现业务流量在加速线路和DDoS高防线路的自动切换，最终将正常流量回送到源站服务器。

操作步骤

1. 登录*DDoS*高防（国际）管理控制台。
2. 将您的网站业务或非网站业务配置接入DDoS高防（国际）保险版/无忧版实例和加速线路实例。

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

   - 网站域名接入DDoS高防（国际）实例：参见网站业务接入*DDoS*高防（国际）防护进行接入配置。您在选择高防独享IP时，需要同时选择DDoS高防（国际）保险版/无忧版实例和加速线路实例的两个独享IP。
   - 业务端口接入DDoS高防（国际）实例：参见非网站业务接入*DDoS*高防（国际）防护进行配置。您需要在DDoS高防（国际）保险版/无忧版实例和加速线路实例中配置转发规则，即分别选择DDoS高防（国际）保险版/无忧版实例和加速线路实例为您的非网站业务配置转发规则。

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

3. 前往流量调度器页面，打开防护调度页签，并单击添加规则。

4. 在添加规则侧边页，设置规则条件，并单击下一步。

   - 联动场景：选择出海加速。
   - 规则名：为规则命名。
   - 高防IP：设置为DDoS高防（国际）保险版/无忧版实例的独享IP。
   - 加速线路IP：设置为DDoS高防（国际）加速线路实例的独享IP。

通过该规则，在业务无攻击的情况下，优先使用加速线路实现快速访问；在遭受攻击的情况下，流量调度器将自动将流量切换至防护线路进行流量清洗。

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

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

5. 在域名解析服务提供商处，修改该域名的DNS解析记录。

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

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

4 用户指南

4.1 接入配置

4.1.1 自定义非标端口

DDoS高防（国际）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DDoS高防（国际）实例。**

端口总数限制

针对每个DDoS高防（国际）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:**
> **DDoS高防（国际）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。**

- **DDoS高防（国际）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, 5111, 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

- DDoS高防（国际）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, 7988, 8443, 9443, 8553, 8663, 9553, 9663, 10050, 10443, 18980, 30050

4.1.2 上传HTTPS证书

要使DDoS高防（国际）帮助您清洗HTTPS业务流量，您必须在网站接入配置中勾选HTTPS协议，并上传HTTPS证书。已上传证书发生变化时，您也要在DDoS高防（国际）控制台及时更新证书。

前提条件

- 已完成网站业务接入配置（具体操作请参见网站业务接入DDoS高防（国际）防护）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DDoS高防（国际）管理控制台。
2. 在左侧导航栏，单击接入配置 > 网站接入。
3. 在接入配置列表中，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_32*。

   - 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，请参见*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。

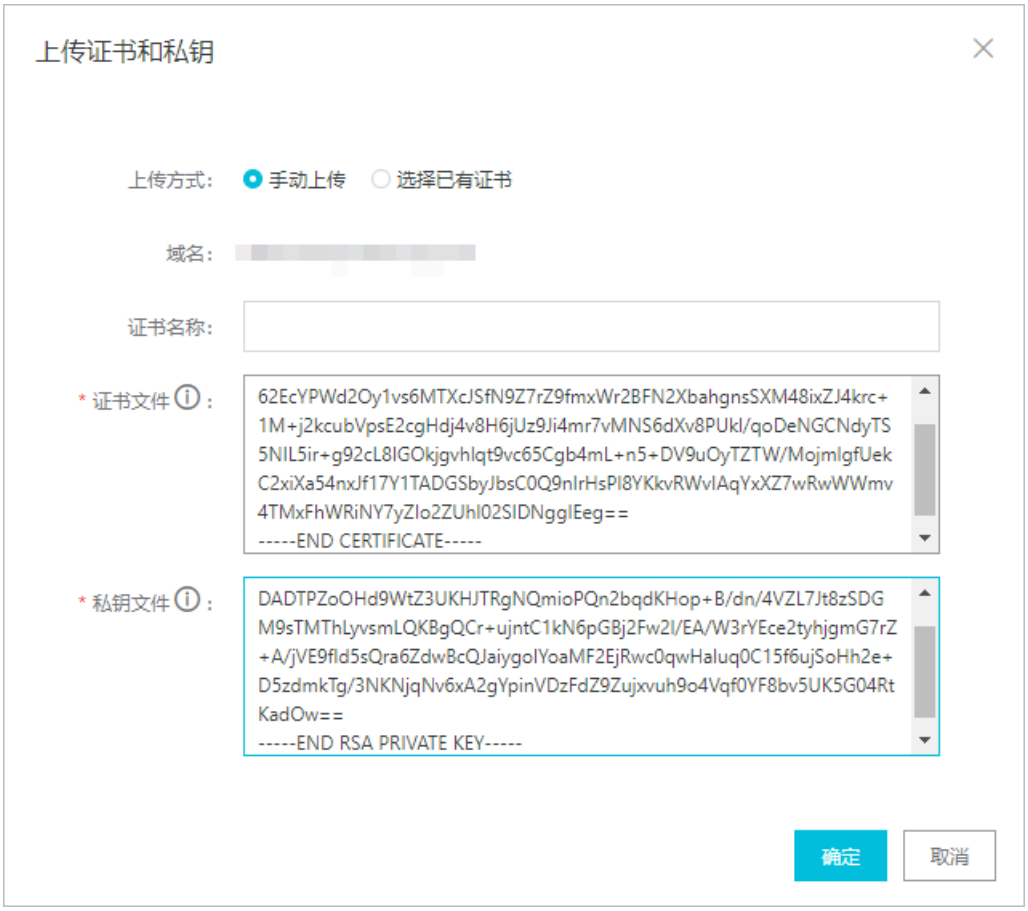
     证书文件文本内容样例

     ```
     -----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。

4.1.3 自定义TLS安全策略

DDoS高防（国际）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DDoS高防（国际）实例。

- 已添加网站接入配置（具体操作请参见网站业务接入*DDoS*高防（国际）防护）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。

操作步骤

1. 登录*DDoS*高防（国际）管理控制台。
2. 在左侧导航栏，单击接入配置 > 网站接入。
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

4.1.4 流量调度器

DDoS高防（国际）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、出海加速功能。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（国际）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。 
出海加速	使用DDoS高防（国际）防护业务，无攻击时，业务使用加速IP；被攻击时，需要切换到DDoS高防。	无攻击时，使用加速线路IP；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。

功能	限制条件	说明
	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。
出海加速	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。
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。

功能	配置说明
出海加速	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，参见添加防护调度规则。 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。
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（国际）控制台。
2. 在左侧导航栏，单击流量调度器。
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： · 出海加速 · 云产品联动 · 阶梯防护（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。
加速线路IP	在出海加速场景下，选择要联动的加速线路IP。

配置项	说明
云资源	在云产品联动和阶梯防护场景下，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。

图 4-1: 出海加速配置示例

图 4-2: 阶梯防护配置示例

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（国际）控制台。
2. 在左侧导航栏，单击流量调度器。
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高防（国际）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。

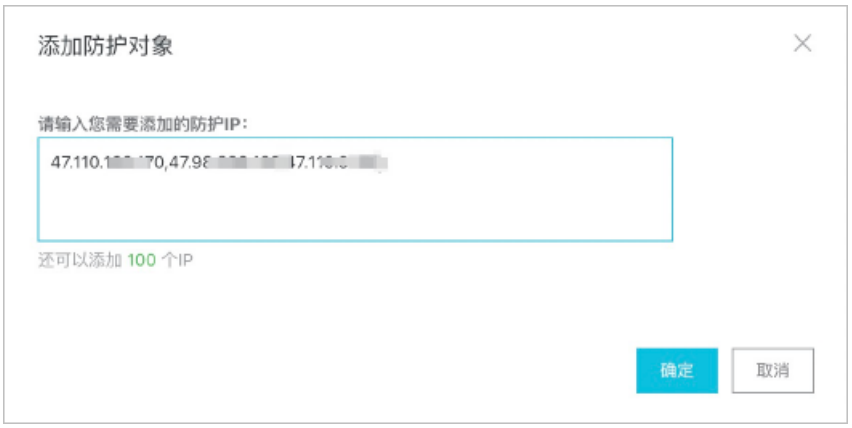
成功添加联动，调度器为新建规则分配一个CNAME地址。要使调度规则生效，您需要前往云资源的DNS服务商处修改其DNS解析，应用CNAME解析并将解析目标设置为调度器分配的CNAME地址。

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。

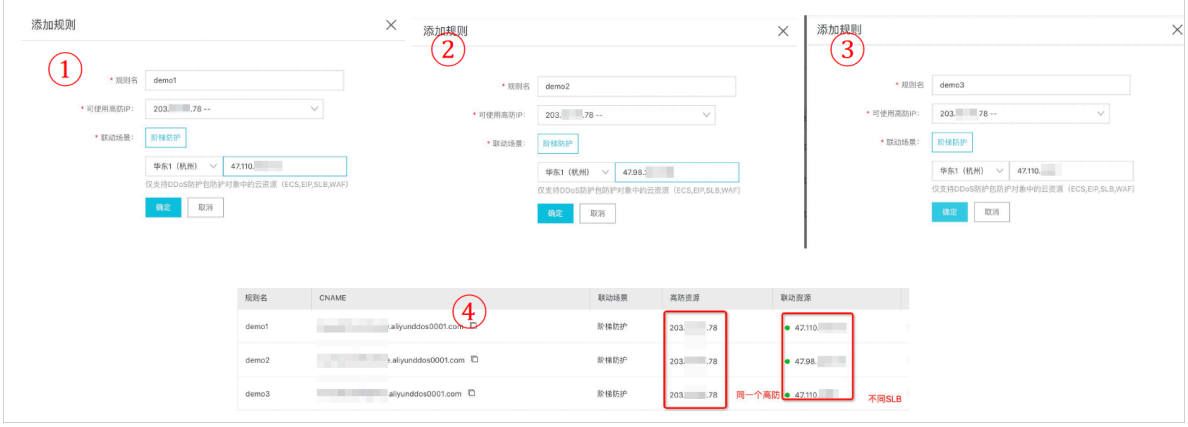
多路分摊切换配置示例

以多防护包切换DDoS高防（国际）为例，介绍云产品与DDoS高防（国际）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。

4.1.5 CNAME复用

若您在同一个服务器上有多个网站域名需要接入DDoS高防（国际），您可以申请开通CNAME复用，实现只添加一次高防配置，而使高防配置的CNAME地址供多个域名复用。启用CNAME复用后，您只需将同服务器上多个域名的解析指向高防CNAME地址，即可将多个域名接入高防，无需为每个域名分别添加高防配置。

使用场景

CNAME复用适用于以下场景：

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

使用限制

下表描述了CNAME复用的使用限制。

限制条件	说明
协议类型	仅支持HTTP协议，不支持HTTPS协议。
源站	复用CNAME的一组域名必须对应同一个源站。

前提条件

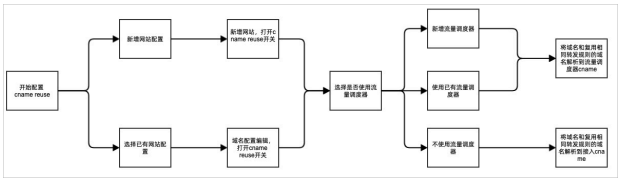
CNAME复用需要申请开放后才能使用。若有相关需求，请通过工单提交申请。本文操作描述建立在已开放CNAME复用的前提下。

启用CNAME复用

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

- **若结合流量调度器使用，则需要关联对应的防护调度规则，且域名解析中将复用防护规则的CNAME地址。**
- **若不使用流量调度器，则域名解析中将复用高防网站配置的CNAME地址。**

下图描述了CNAME复用的配置流程。



为便于后续操作描述，做以下假设：

- **源站服务器有两个IP：1.1.1.1、2.2.2.2。**
- **源站（1.1.1.1）有三个域名：a.test、b.test、c.test。**
- **DDoS高防实例IP：9.9.9.9。**

以下操作描述了使用CNAME复用，将一个源站IP（1.1.1.1）下多个域名（a.test、b.test、c.test）接入DDoS防护（国际）的配置方法。

1. 在网站配置中启用CnameReuse。

   a) 登录云盾DDoS高防（国际）控制台。

   b) 前往接入配置页面，打开网站接入页签。

   c) 添加一个网站配置或者编辑已有网站配置，在网站配置中启用CnameReuse。关于添加网站配置的具体操作，请参见网站业务接入DDoS高防（国际）防护。

   示例：源站IP是1.1.1.1，网站是a.test（也可以是b.test、c.test），DDoS高防（国际）IP是9.9.9.9。

2. 选择是否结合流量调度器及更新域名CNAME解析。

   在启用CnameReuse时，您需要选择是否结合流量调度器。

   - 不使用流量调度器

     a. 在选择是否结合流量调度器对话框中，选择不使用流量调度器，并单击完成。

     b. 成功添加网站配置后，记录网站配置的CNAME地址。

     c. 前往域名服务商，更新源站（1.1.1.1）对应的所有网站（a.test、b.test、c.test）的域名解析，应用CNAME解析并将记录值更新为网站配置的CNAME地址。

   - 使用流量调度器

     a. 在选择是否结合流量调度器对话框中，选择使用流量调度器，并选择对应的流量调度规则，单击完成。

流量调度器规则应联动网站配置中用到的源站IP（1.1.1.1）和高防IP（9.9.9.9）。若您还未创建对应规则，请单击新建流量调度规则添加对应规则（见下图示例），再选择应用规则。

b. 成功选择流量调度器规则后，记录调度规则的CNAME地址。

c. 前往域名服务商，更新源站（1.1.1.1）对应的所有网站（a.test、b.test、c.test）的域名解析，应用CNAME解析并将记录值更新为调度规则的CNAME地址。

3. （可选）若仍需要为不同源站（2.2.2.2）对应的域名接入DDoS防护，请重复步骤1~2进行配置。

关闭CNAME复用

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

注意:

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

1. 登录云盾DDoS高防（国际）控制台。
2. 前往接入配置页面，打开网站接入页签。
3. 编辑已有网站配置，并在网站配置中关闭Cname Reuse。
4. 根据需要选择是否保留网站配置和防护调度规则。
   - 若保留网站配置，则网站配置中的转发逻辑继续生效。
   - 若保留防护调度规则，则流量调度器继续生效。

4.2 网络七层防护配置

4.2.1 设置网站访问黑白名单

DDoS高防（国际）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DDoS高防（国际）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DDoS高防（国际）管理控制台。
2. 定位到接入配置 > 网站接入页面，选择已接入防护的域名，单击CC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DDoS高防（国际）实例生效。

4.2.2 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DDoS高防（国际）实例。

背景信息

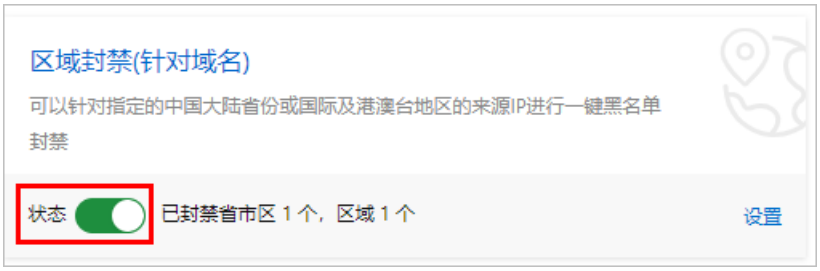
假设example.aliyundemo.com域名的正常用户均来自中国大陆（含港澳台特别行政区），您可以为example.aliyundemo.com域名配置区域封禁，封禁来自海外地区（亚洲，欧洲，北美洲，南美洲，非洲，大洋洲，南极洲）的访问请求。

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DDoS高防（国际）中识别过滤，并不能减小进入DDoS高防网络的攻击流量。

操作步骤

1. 登录*DDoS*高防（国际）管理控制台。
2. 定位到防护设置 > 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。

4.2.3 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。

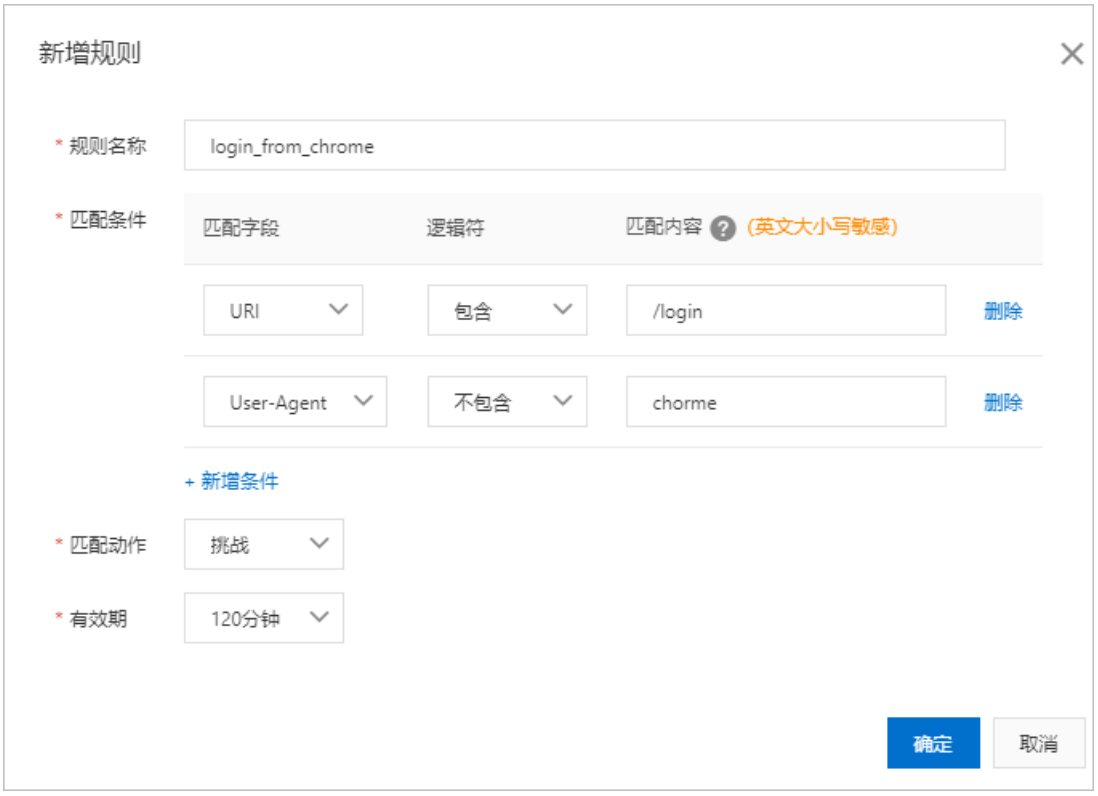
注意事项

- 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*DDoS*高防（国际）管理控制台。
2. 定位到防护设置 > 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DDoS高防（国际）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

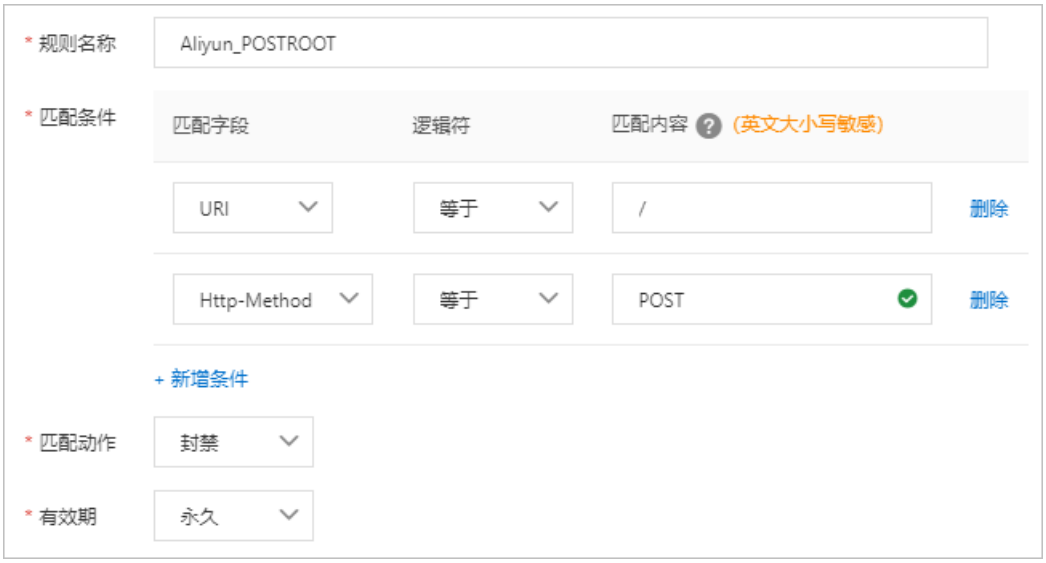
匹配字段	字段描述	适用逻辑符
params	访问请求的URL地址中的参数部分，通常指URL中”?”后面的部分。例如，www.abc.com/index.html?action=login中的action=login就是参数部分。	· 包括 · 不包括 · 等于 · 不等于 · 长度小于 · 长度等于 · 长度大于

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。

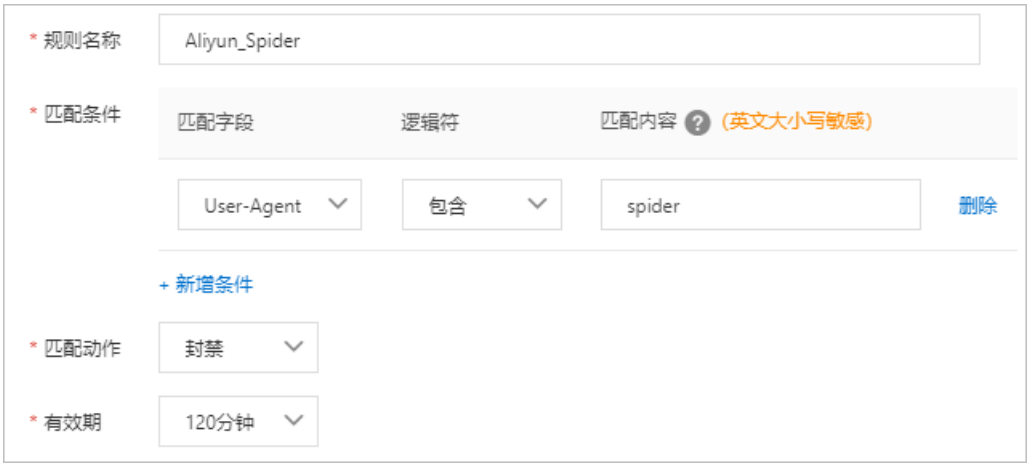
· **拦截特定的攻击请求**

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。

4.2.4 防护HTTP(S) Flood攻击

DDoS高防（国际）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DDoS高防（国际）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*DDoS高防（国际）管理控制台*。**
2. **定位到接入配置 > 网站接入页面，选择已接入防护的网站域名配置记录，单击CC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。**

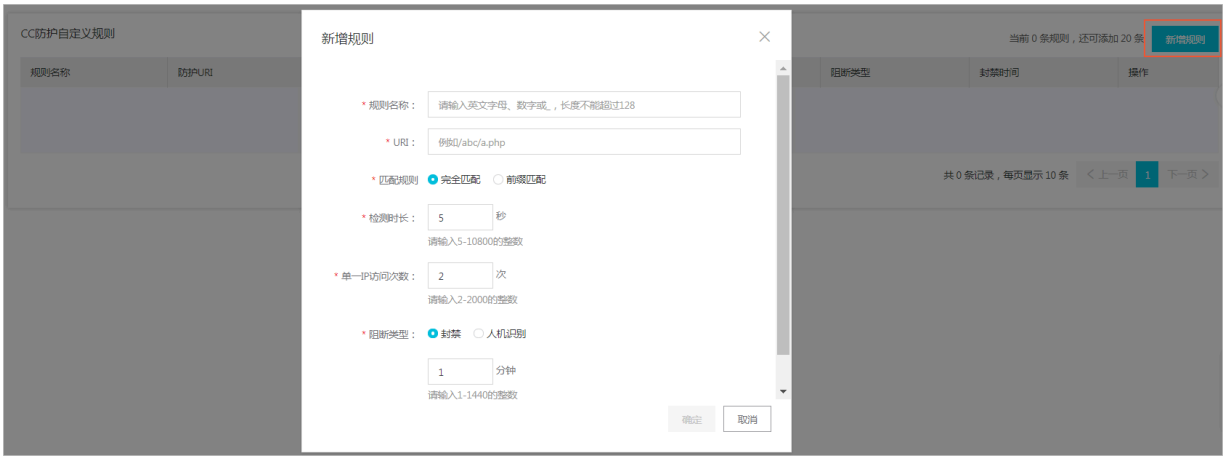
说明:

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

DDoS高防（国际）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。

4.2.5 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。

背景信息

注意:

开启AI智能防护时，自动下发的智能规则无法手动删除。若智能防护规则不适合您的业务场景，建议您关闭智能防护开关。关闭AI智能防护后，AI产生的防护规将即时清空。

操作步骤

1. **登录*DDoS*高防（国际）管理控制台。**
2. **定位到防护设置 > 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。
- 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。

预期结果

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，具体规则条目在**精准访问控制规则**模块中查看。AI智能防护规则的名称以“smartcc_”开头。

说明:

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，防护规则会自动失效并清除。

4.2.6 加速网站静态页面访问

DDoS高防（国际）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DDoS高防（国际）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DDoS高防（国际）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*DDoS高防（国际）管理控制台*。**
2. **定位到防护设置 > 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。

4.2.7 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DDoS高防（国际）直接攻击源站。您可以在DDoS高防（国际）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*DDoS*高防（国际）管理控制台。
2. 定位到接入配置 > 网站接入页面。
3. 单击更换ECS IP。

警告:
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。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。

   说明:
   若您已将需要更换IP的ECS停机，请直接跳过本步骤。

   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DDoS高防（国际）后面，不要对外暴露。

4.3 网络四层防护配置

4.3.1 设置DDoS防护策略

DDoS高防（国际）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

DDoS高防（国际）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DDoS高防（国际）实例的非网站业务的“IP+端口”的连接速度、包长度等参数进行限制，实现缓解小流量的连接型攻击的防护能力。

DDoS高防（国际）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：

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。

DDoS防护策略配置项	说明
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。
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*DDoS高防（国际）管理控制台*。
2. 定位到接入配置 > 非网站接入页面，选择DDoS高防（国际）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。

4.3.2 设置健康检查规则

DDoS高防（国际）为已接入防护的非网站业务提供健康检查功能。

DDoS高防（国际）的非网站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DDoS高防（国际）实例的IP和端口提供健康检查功能。

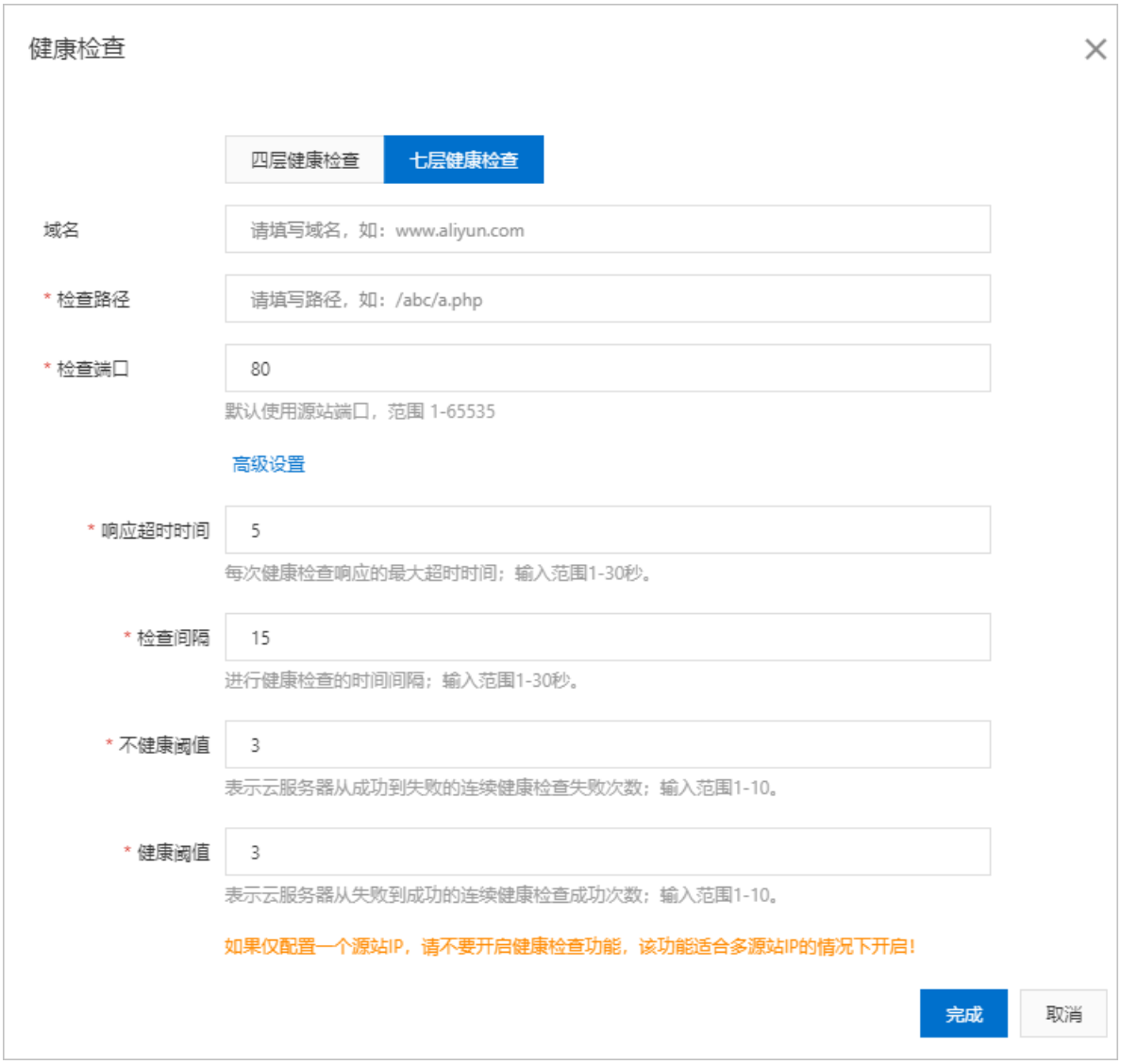
您可以针对指定IP的指定端口设置健康检查规则。

操作步骤

1. 登录*DDoS高防（国际）管理控制台*。

2. 定位到接入配置 > 非网站接入页面。
3. 选择DDoS高防（国际）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。
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。

健康检查配置	说明
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。

4.3.3 设置会话保持规则

DDoS高防（国际）为已接入防护的非网站业务提供会话保持功能，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

DDoS高防（国际）的非网站业务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DDoS高防（国际）实例的IP和端口提供会话保持功能。

操作步骤

1. 登录*DDoS高防（国际）管理控制台*。
2. 定位到接入配置 > 非网站接入页面。
3. 选择DDoS高防（国际）实例。
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 查看安全总览

在将业务接入DDoS高防（国际）服务并切换业务流量至高防实例后，您可以在DDoS高防（国际）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

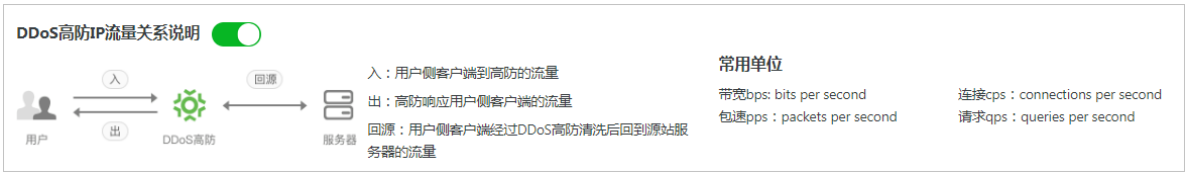
DDoS高防（国际）的安全总览页面向您展示以下业务指标和DDoS攻击事件的概览：

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

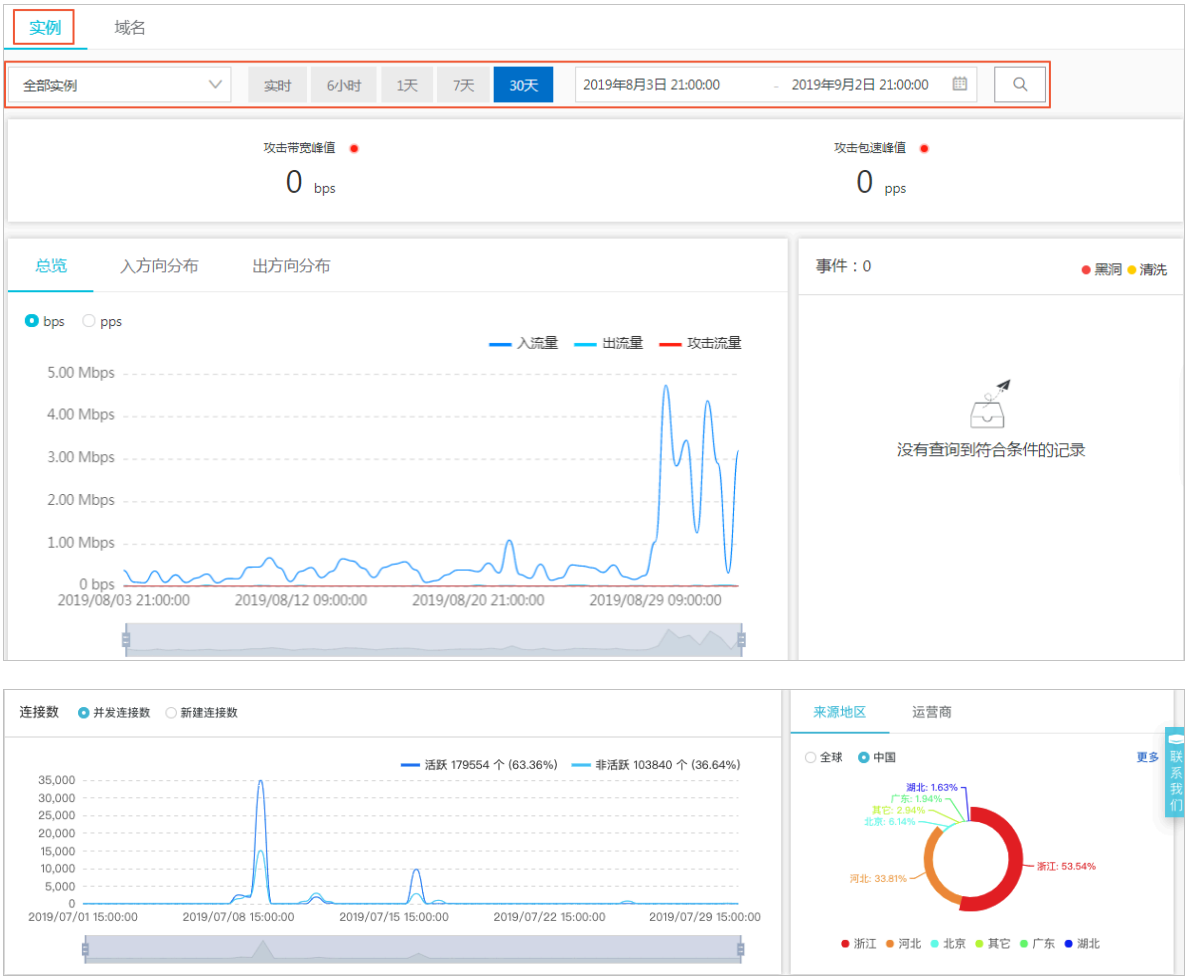
操作步骤

1. 登录*DDoS*高防（国际）管理控制台。
2. 定位到安全总览页面，查看并熟悉DDoS高防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. 选择实例页签，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

  将鼠标移至被攻击的IP或端口上，将展示被攻击的IP和端口信息、攻击的类型和峰值、防护结果。

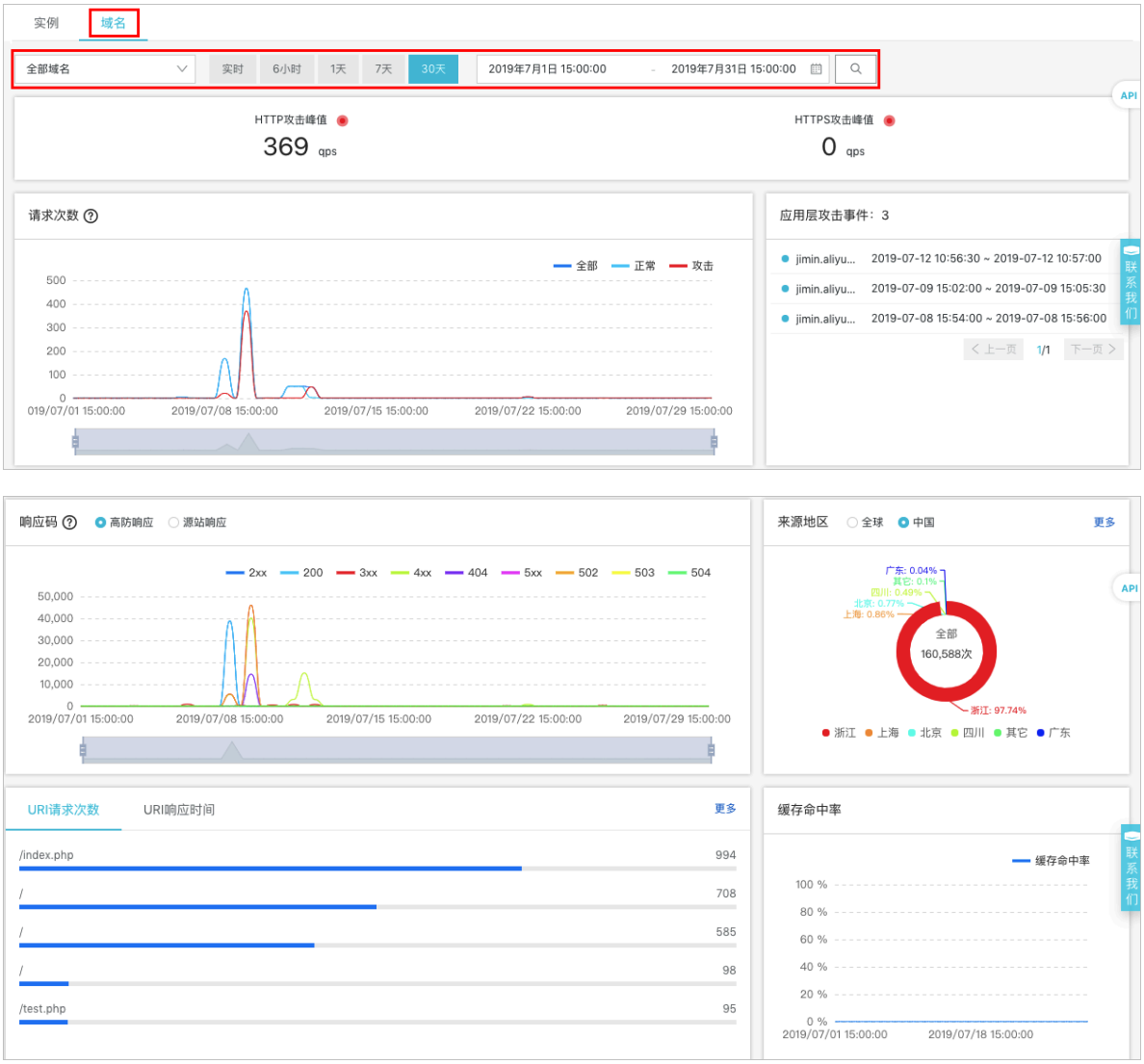
- （端口）连接数
  - 并发连接数：客户端同一时间与高防建立的TCP连接数量
  - 新建连接数：客户端每秒内新增的与高防通信的TCP连接数

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. 选择域名页签，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

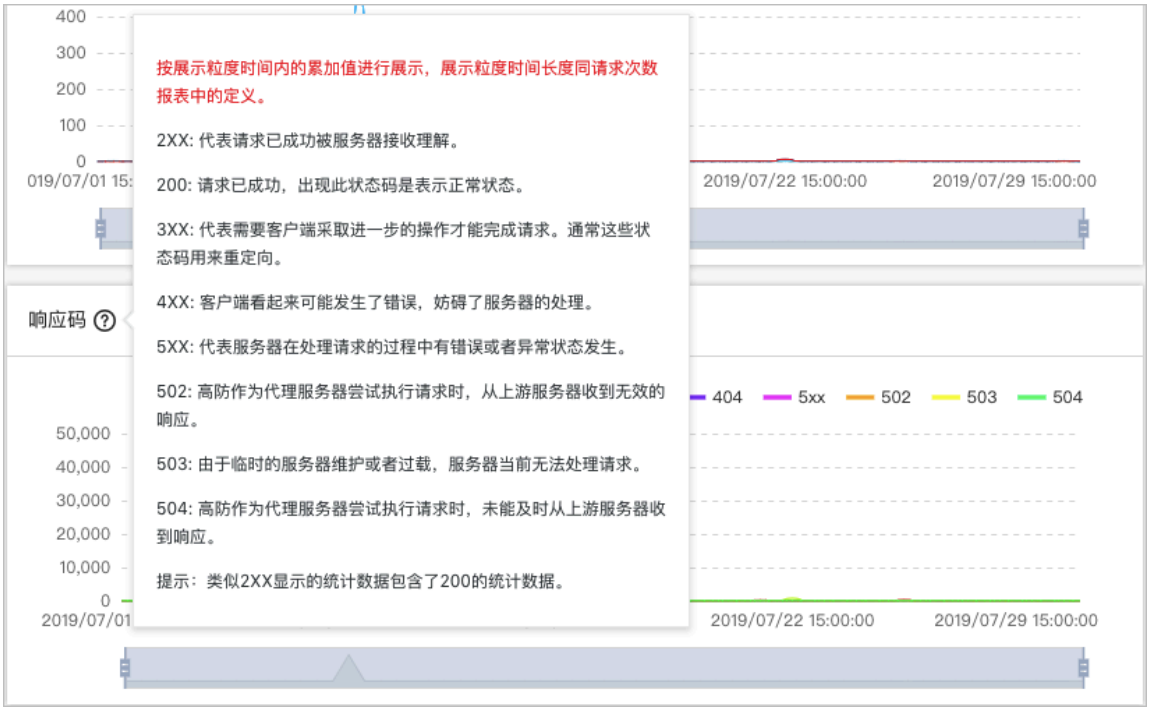
  请求次数趋势图按峰值展示，不同的查询时间间隔对应的展示粒度不同，具体如下：

  - 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

将鼠标移动至被攻击的域名上，将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。

4.5 业务配置批量导入导出

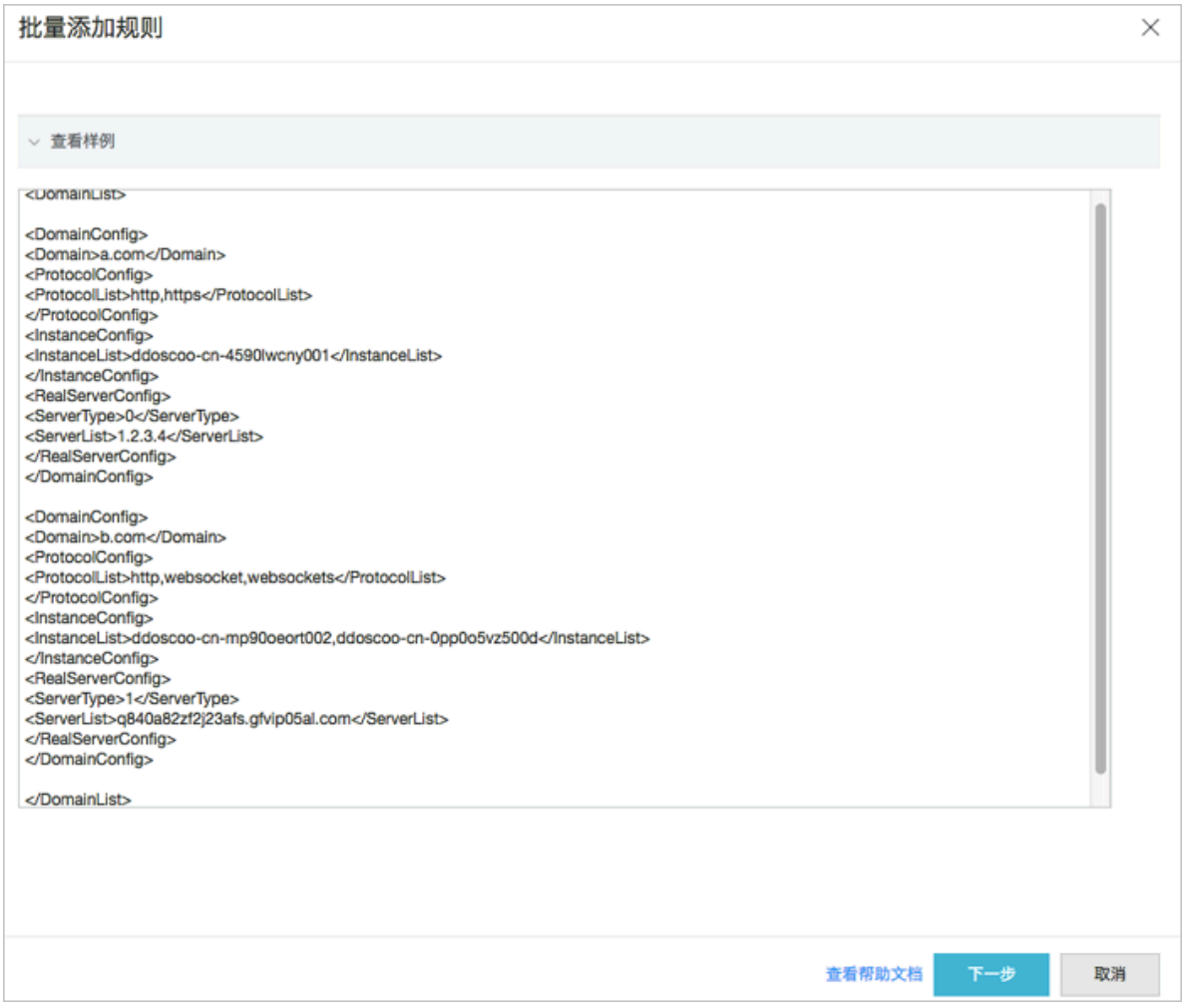
当您的网站域名配置或四层转发规则配置数量过多时，如果您需要保存当前时间点的业务接入配置或进行配置迁移，您可以通过业务配置的批量导入/导出功能，快速完成这类操作。

- **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. **登录云盾高防（国际）控制台。**
2. **定位到接入配置 > 网站接入页面，在域名配置列表下方单击批量导入，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。

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DDoS高防（国际）实例。 说明: 由于每个DDoS高防（国际）实例对应一个独享高防IP，只需填写DDoS高防（国际）实例的实例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>ddosDip-cn-v0h0v9a3x07</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>ddosDip-cn-v0h0v9a3x07,ddosDip-cn-0pp0u9slr01</
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. **定位到接入配置 > 网站接入页面，在域名配置列表下方单击批量导出。**
2. **单击确定，即开始执行域名配置导出任务。**
3. **单击接入配置页面右上角的任务进度按钮，查看导出任务下载进度。**
4. **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. **定位到接入配置 > 非网站接入页面。**
2. **在转发规则列表下方选择批量添加 > 添加转发规则，一次性配置多条转发规则。**

> **说明:**
> **您也可以选择添加会话保持/健康检查配置或添加DDoS防护策略，批量添加相应规则配置。**

3. **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**

     ```
     tcp 90 91 192.136.12.41
     udp 22 13 12.14.1.23,10.23.4.12
     ```

     字段含义从左至右以此为协议、转发端口、源站端口、源站IP。

   - **添加会话保持/健康检查配置**

```
8081 tcp 4000 tcp 22 5 5 3 3
8080 tcp 4000 http 22 5 5 3 3 /search.php www.baidu.com
```

字段含义从左至右依次为转发协议端口、转发协议、会话保持超时时间、健康检查类型、检查端口、检查超时时间、检查间隔、不健康阈值、健康阈值、检查路径（http时必选）、域名（http时可选）。

- 添加DDoS防护策略

```
8081 tcp 2000 50000 20000 100000 1 1500 on on
8080 udp 1000 50000 20000 100000 1 1500
```

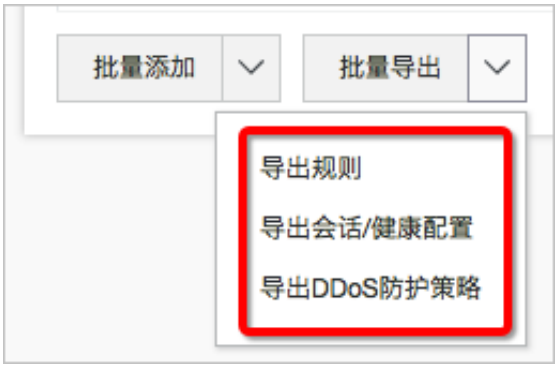
字段含义从左至右以此为转发协议端口、转发协议、源新建连接限速、源并发连接限速、目的新建连接限速、目的并发连接限速、包长度最小值、包长度最大值、虚假源与空连接（仅TCP协议时生效，空连接开启前需要先开启虚假源）。

4. 单击确定，即可将相关配置导入。

批量导出转发规则配置

1. 定位到接入配置 > 非网站接入页面。
2. 在转发规则列表下方选择批量导出 > 导出转发规则。

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



3. 在确认提示单框中，击确定，即可导出当前转发规则配置。
4. 单击接入配置页面右上角的任务进度按钮，查看导出任务下载进度。
5. 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。

4.6 全量日志

DDoS高防（国际）的网站访问日志（包含CC攻击日志）与阿里云日志服务联动，为您提供全量日志服务。全量日志为增值服务，需要开通后使用。开通全量日志，则日志服务实时采集接入DDoS高防（国际）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。

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并附加防护策略就显得尤其重要。

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

阿里云日志服务（Log Service，简称 LOG）是针对日志类数据的一站式服务，在阿里巴巴集团经历大量大数据场景锤炼而成。您无需开发就能快捷完成日志数据采集、消费、投递以及查询分析等功能，提升运维、运营效率，建立DT时代海量日志处理能力。更多信息，请参见什么是日志服务。

开通全量日志服务

1. 登录*DDoS*高防（国际）管理控制台。
2. 定位到全量日志页面，单击立即购买。
3. 在全量日志服务购买页面，将适用产品设置为DDoS高防（国际），并根据您的业务需要，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。

   DDoS高防（国际）全量日志服务的单价为1000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）。

4. **单击立即购买，完成支付。**
5. **回到DDoS高防（国际）DDoS高防（国际）控制台，在统计 > 全量日志页面，单击立即授权。**

6. 在云资源访问授权页面中，单击同意授权，授权DDoS高防（国际）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，您可以在日志服务页面单击规格详情，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。
- 当日志存储空间长期空闲时，您也可以根据实际日志量的大小，降低日志存储规格。

为网站启用全量日志

1. 登录*DDoS*高防（国际）管理控制台。
2. 定位到全量日志页面。
3. 在日志服务页面，选择网站域名，开启其状态开关，为网站域名启用全量日志。
   启用全量日志后，您可以在日志服务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DDoS高防（国际）服务的日志分析与日志报表功能，请参见查看日志报表和日志分析。

使用全量日志

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，请参见下文常用查询语句示例。	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，全量日志服务默认为您提供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

全量日志应用场景

全量日志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：

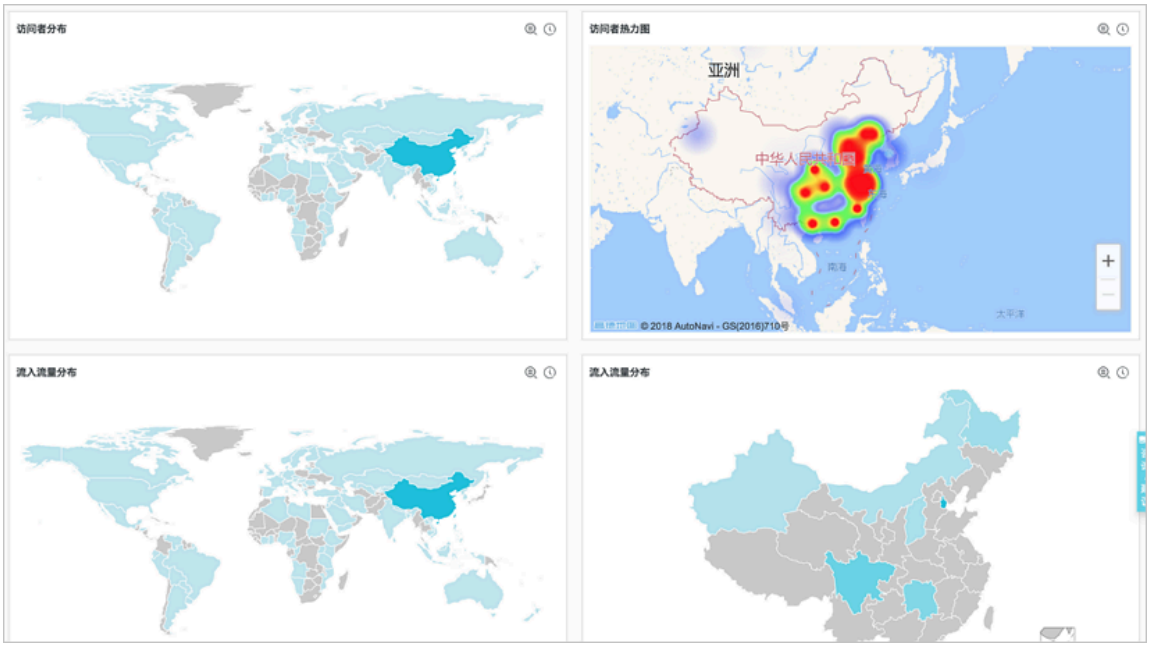
  ```
  __topic__: DDoS_access_log
  ```

- **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。

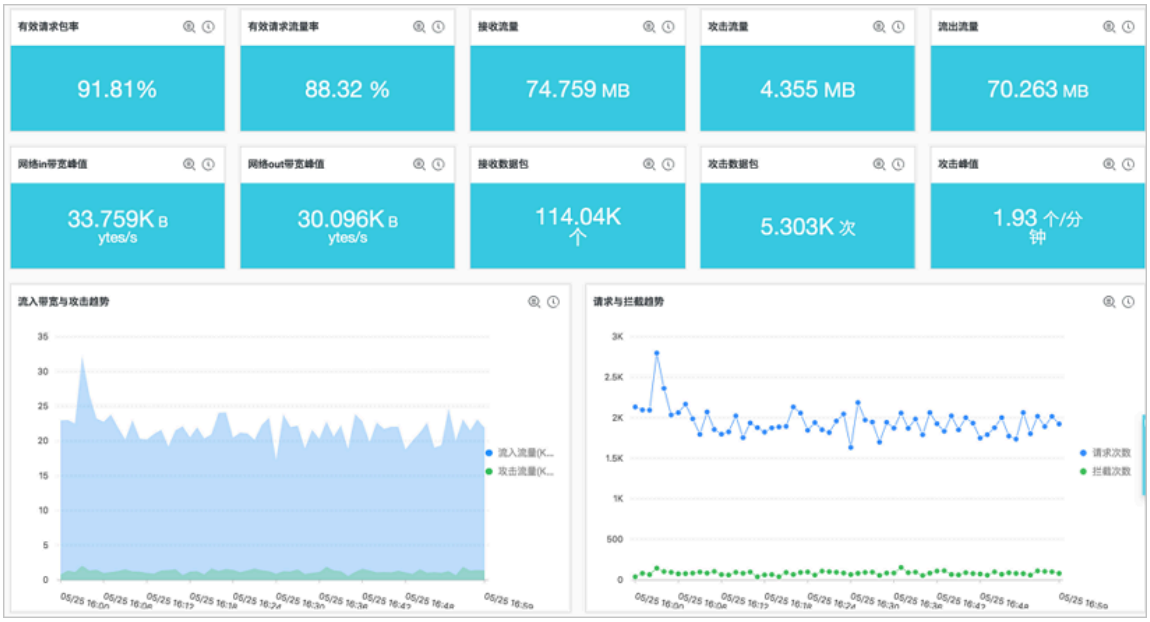
  - **例如，通过以下语句分析DDoS访问日志中记录的CC攻击者国家分布：**

    ```
    __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
    ```

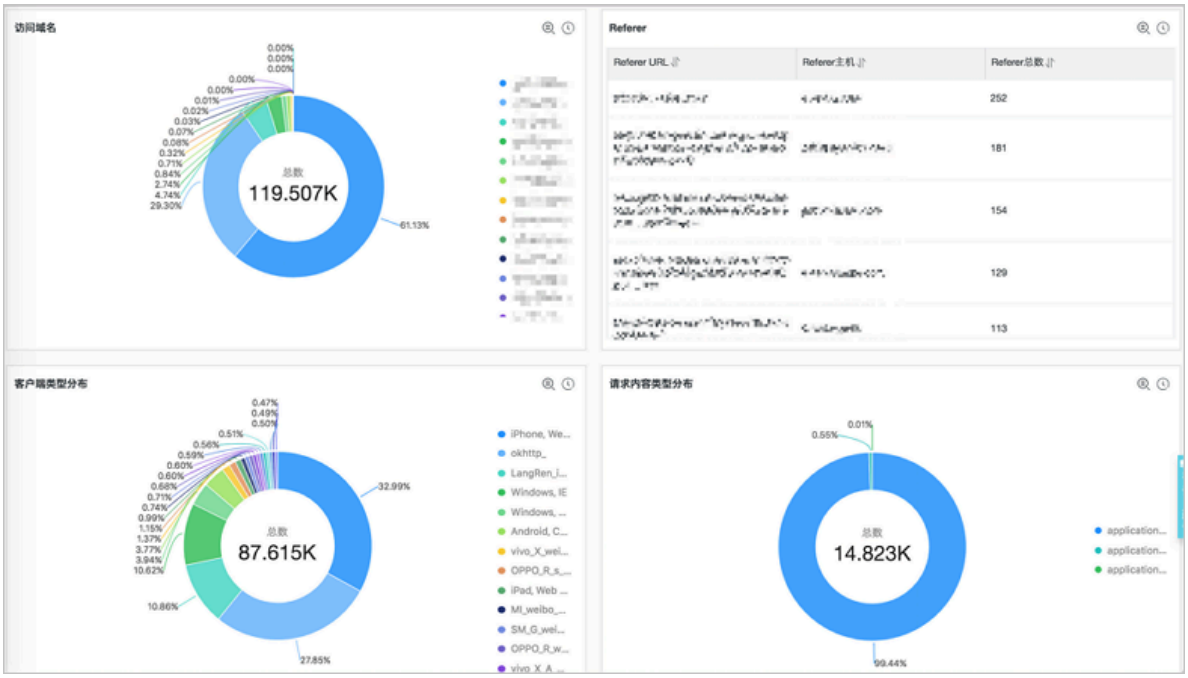
    

- **网站运营分析**

  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

4.7 全量日志字段说明

DDoS高防（国际）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。	-
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

字段	说明	示例
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
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

字段	说明	示例
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
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

字段	说明	示例
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

4.8 查看日志报表

日志报表页面内嵌了日志服务的仪表盘页面。该页面为您展示您的默认仪表盘，您可以在当前页面通过修改时间范围、添加过滤条件等操作，查看多种筛选条件下的仪表盘数据。

进入仪表盘

为网站域名开启全量日志后，您可以单击日志报表，查看内置的DDoS防护仪表盘。

图 4-3: 查看报表

日志服务为您自动创建两个默认的仪报表，即运维中心和访问中心。

仪表盘名称	说明
运维中心	展示高防保护的网站目前的总体运营状况，包括有效请求状况、流量、趋势以及被CC攻击的流量、峰值、攻击者分布等数据。
访问中心	展示高防保护的网站目前的总体被访问状况，包括PV/UV趋势与带宽峰值、访问者分布、流量线路分布、客户端类型分布、请求分布、被访问网站分布等数据。

图 4-4: 默认仪表盘

除了查看报表之外，您还可以进行以下操作：

- **选择时间范围。**
- **查看图表。**

时间选择器

仪表盘页面的所有图表都是基于不同时间段的数据统计结果，例如访问量的默认时间范围为1天，访问趋势为30天。如您想要设置当前页面的所有图表均按照同样的时间范围显示，可以设置时间选择器。

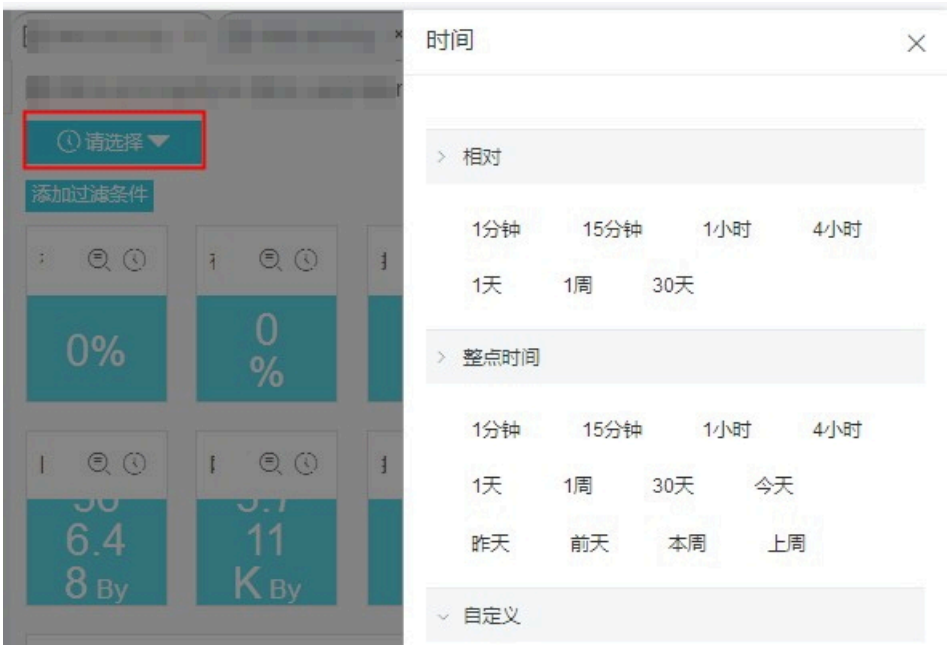
操作步骤

1. **单击请选择。**
2. **在弹出的设置框中选择您的设置。您可以选择相对时间、整点时间或设置自定义时间。**

说明:

- **修改时间范围后，所有图表的时间都会改成这个时间范围。**
- **时间选择器仅在当前页面提供临时的图表查看方式，系统不保存该设置。您下次查看报表时，系统仍会为您展示默认的时间范围。**

图 4-5: 设置时间范围



图表类型

报表展示区域按照预定义的布局展示多个报表，包括如下几个类型，更多图表类型请参见*#unique_61*。

图表类型	说明
数字	表示一些重要指标，如有效请求率、攻击峰值等。
线/面积图	表示一些重要指标特定时间单元内的趋势图，如流入带宽趋势、攻击拦截趋势等。
地图	表示一些访问者、攻击者的地理分布，如CC攻击者国家分布、访问热点分布等。
饼图	表示一些信息的分布，例如被攻击网站前10、客户端类型分布等。
表格	展示攻击者列表等信息，一般分多个列。
地图	表示一些数据的地理分布。

默认仪表盘

- **运维中心：展示高防保护的网站目前的总体运营状况，包括有效请求状况、流量、趋势以及被CC攻击的流量、峰值、攻击者分布等。**

图表	类型	默认时间范围	描述	样例
有效请求包率	单值	1小时（相对）	有效请求，即非CC攻击或400错误的请求个数在所有请求总数的占比。	95%
有效请求流量率	单值	1小时（相对）	有效请求在所有请求总流量的占比。	95%
接收流量	单值	1小时（相对）	有效请求流入流量总和，单位MB。	300 MB
攻击流量	单值	1小时（相对）	CC攻击的流入流量总和，单位MB。	30 MB
流出流量	单值	1小时（相对）	有效请求流出流量总和，单位MB。	300 MB
网络in带宽峰值	单值	1小时（相对）	网站请求的流入流量速率的最高峰值，单位为Bytes/s。	100 Bytes/s
网络out带宽峰值	单值	1小时（相对）	网站请求的流出流量速率的最高峰值，单位为Bytes/s。	100 Bytes/s
接收数据包	单值	1小时（相对）	有效请求（非CC攻击）的流入请求个数，单位为个。	30000 个
攻击数据包	单值	1小时（相对）	CC攻击的请求个数总和，单位为个。	100 个

图表	类型	默认时间范围	描述	样例
攻击峰值	单值	1小时（相对）	CC攻击的最高峰值，单位为个/峰值。	100 个/分钟
流入带宽与攻击趋势	双线图	1小时（整点）	每分钟的有效请求和攻击请求的流量带宽的趋势图。单位为KB/s。	-
请求与拦截趋势	双线图	1小时（整点）	每分钟的请求和拦截的CC攻击请求总数的趋势图。单位为个/分钟。	-
有效请求率趋势	双线图	1小时（整点）	每分钟的有效请求（非CC攻击或400错误的请求）个数在所有请求总数的占比趋势图。	-
访问状态分布趋势	流图	1小时（整点）	每分钟的各种请求处理状态（400、304、200等）的趋势图单位为个/分钟。	-
CC攻击者分布	世界地图	1小时（相对）	CC攻击的次数总和在来源国家的分布。	-
CC攻击者分布	中国地图	1小时（相对）	CC攻击的次数总和在来源省份（中国）的分布。	-
攻击者列表	表格	1小时（相对）	前100个攻击最多的攻击者信息，包括IP、地域城市、网络、攻击次数和攻击总流量。	-

图表	类型	默认时间范围	描述	样例
攻击接入线路分布	饼图	1小时（相对）	CC攻击来源的接入高防线路分布，如电信、联通和BGP等。	-
被攻击网站Top10	环图	1小时（相对）	被攻击最多的10个网站。	-

- 访问中心：展示高防保护的网站目前的总体被访问状况，包括PV/UV趋势与带宽峰值、访问者分布、流量线路分布、客户端类型分布、请求分布、被访问网站分布等。

图表	类型	默认时间范围	描述	样例
PV	单值	1小时（相对）	请求总数。	100000
UV	单值	1小时（相对）	独立的访问客户端总数。	100000
流入流量	单值	1小时（相对）	网站的流入流量总和，单位为MB。	300 MB
网络in带宽峰值	单值	1小时（相对）	网站请求的流入流量速率的最高峰值，单位为Bytes/s。	100 Bytes/s
网络out带宽峰值	单值	1小时（相对）	网站请求的流出流量速率的最高峰值，单位为Bytes/s。	100 Bytes/s
流量带宽趋势	双线图	1小时（整点）	每分钟的网站流入流出流量的趋势图（单位KB/S）	-
请求与拦截趋势	双线图	1小时（整点）	每分钟的请求和拦截的CC攻击请求总数的趋势图。单位为个/分钟。	-
PV/UV访问趋势	双线图	1小时（整点）	每分钟的PV与UV的趋势图。单位为个。	-
访问者分布	世界地图	1小时（相对）	访问者PV在来源国家的分布。	-

图表	类型	默认时间范围	描述	样例
访问者热力图	高德地图	1小时（相对）	访问者在地理位置上的访问热力图。	-
流入流量分布	世界地图	1小时（相对）	流入流量总和在来源国家的分布。单位为MB。	-
流入流量分布	中国地图	1小时（相对）	流入流量总和在来源省份的分布。单位为MB。	-
接入线路分布	环图	1小时（相对）	访问者来源的接入高防线路分布，如电信、联通和BGP等。	-
流入流量网络提供商分布	环图	1小时（相对）	访问者通过网络运营商接入的流入流量分布。如电信、联通、移动、教育网等。单位为MB。	-
访问最多的客户端	表格	1小时（相对）	前100个访问最多的客户端信息，包括IP、地域城市、网络、请求方法分布、流入流量、错误访问次数、拦截的CC攻击次数等。	-
访问域名	环图	1小时（相对）	前20个被访问最多的域名。	-
Referer	表格	1小时（相对）	前100个最多的跳转Referer URL、主机以及次数等。	-

图表	类型	默认时间范围	描述	样例
客户端类型分布	环图	1小时（相对）	前20个被访问最多的User Agent（用户代理），如iPhone、iPad、Widnows IE、Chrome等。	-
请求内容类型分布	环图	1小时（相对）	前20个最多的请求内容类型，如HTML、Form、JSON、流数据等。	-

4.9 日志分析

全量日志页面嵌入了日志服务全量日志和日志报表页面。开通全量日志功能后，您可以在当前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。

进入日志查询页面

为网站域名开启全量日志后，您可以单击全量日志，进入日志查询页面。

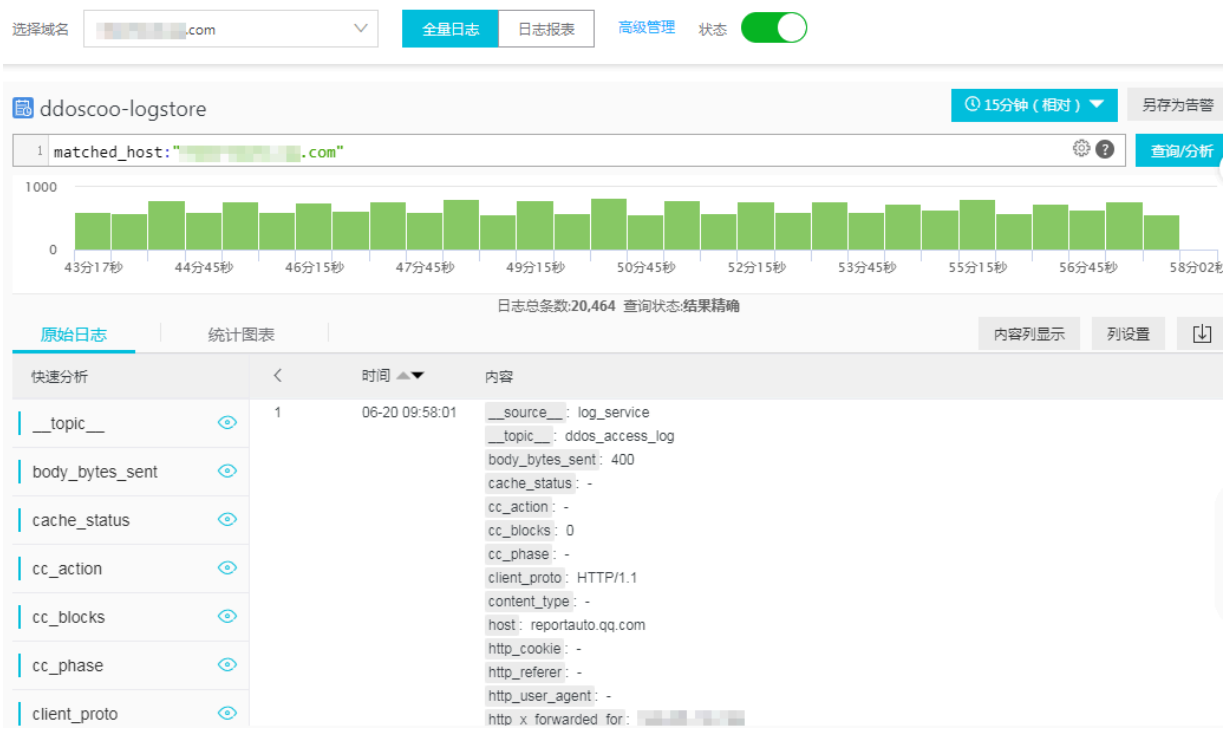
图 4-6: 全量日志

在查询页面，输入您的查询分析语句，选择日志时间范围后单击查询/分析。

说明:

您的高防日志的保存时间为180天，180天之前的日志数据会被删除。默认情况下只能查询到过去180天内的日志数据。

图 4-7: 查询日志



基于查询分析页面，您还可以对查询到的日志数据进行以下操作：

- **自定义查询与分析**

  日志服务定义了一系列查询语法和分析语法，支持多种复杂场景下的日志查询。详情请参见自定义查询与分析。

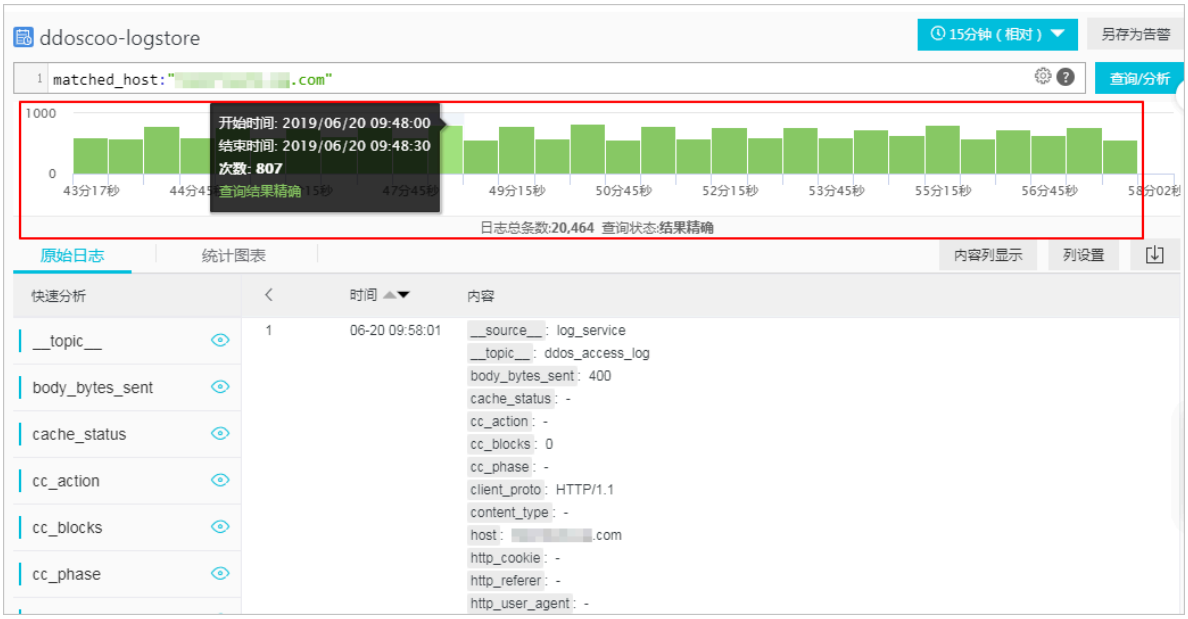
- **查看日志的时间分布**

  搜索框下方展示了符合查询时间和查询语句的日志的时间分布，以时间为横轴、数量为纵轴的柱状图形式展示。并显示查询到的日志总数。

  说明:

可以在柱状图上滑动以选择更小范围的时间区域，时间选择器会自动更新为选择的时间范围，并刷新结果。

图 4-8: 日志的时间分布



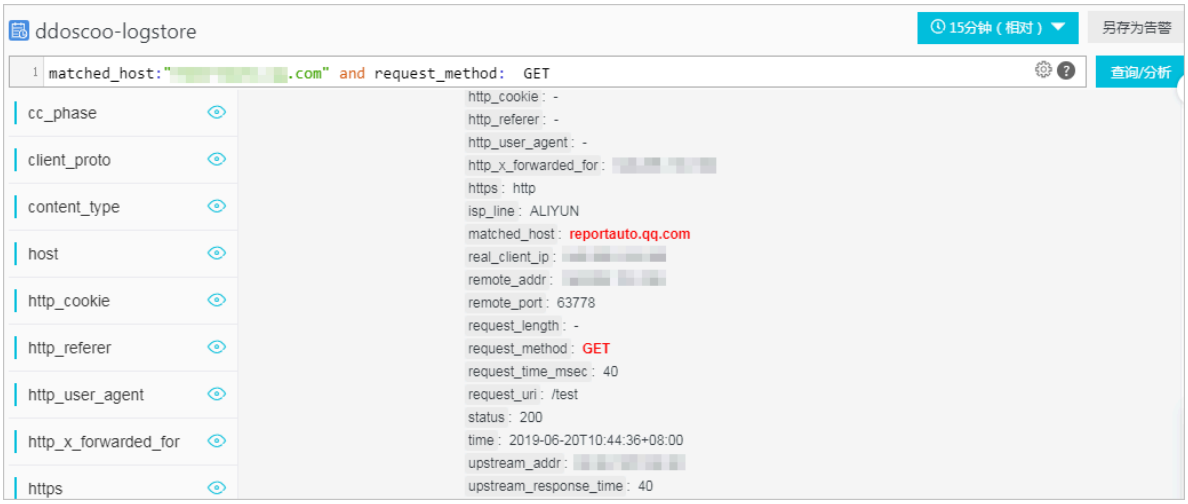
- **查看原始日志**

  原始日志页签中，以分页的形式展示了每一条日志的详细内容，包括时间、内容以及其中的各个字段。您可以对列进行排序、对当前查询结果进行下载，也可以单击列设置，选择特定的字段进行展示等。

  在页面中点击相应字段的值或分词，搜索框中自动输入相应的搜索条件。例如鼠标单击`request_method: GET`中的值`GET`，会自动给搜索框加入如下语句：

  原来的搜索语句 `and request_method: GET`

  图 4-9: 原始日志



- **查看分析图表**

  日志服务支持图表形式展示分析结果，您可以在统计图表页面根据需要选择不同的图表类型。详情请参见分析图表。

  图 4-10: 统计图表

- **快速分析**

  快速分析功能为您提供一键交互式查询体验，帮助您快速分析某一字段在一段时间内的分布情况，减少索引关键数据的时间成本。详细说明请参见快速分析。

  图 4-11: 快速分析

自定义查询分析

日志查询语句由查询语法（Search）和分析语法（Analytics）两个部分组成，中间通过|进行分割：

```
$Search | $Analytics
```

类型	说明
查询（Search）	查询条件，可以由关键词、模糊、数值等、区间范围和组合条件等产生。如果为空或*，则代表所有数据。
分析（Analytics）	对查询结果或全量数据进行计算和统计。

说明：

两部分均为可选，当Search部分为空时代表针对该时间段所有数据不过滤任何条件，直接对结果进行统计。当Analysis部分为空时，代表只返回查询结果，不做统计。

查询语法

日志服务查询语法支持全文查询和字段查询，查询框支持换行显示、语法高亮等功能。

- **全文查询**

  不需要指定字段，直接输入关键字查询。可以用双引号（""）包裹关键字，多个关键字之间以空格或and分割。

  示例：

  - **多关键字查询**

    搜索包含所有www.aliyun.com和error的日志。例如：

    ```
    www.aliyun.com error
    ```

    或者：

    ```
    www.aliyun.com and error
    ```

  - **条件查询**

    这里搜索所有包含www.aliyun.com并且包含error或者404的日志。例如：

    ```
    www.aliyun.com and (error or 404)
    ```

  - **前缀查询**

    这里搜索所有包含www.aliyun.com并且包含failed_开头关键字。例如：

    ```
    www.aliyun.com and failed_*
    ```

    说明：

    查询只支持后缀加*，不支持前缀*，如：*_error。

- **字段查询**

  日志服务支持基于字段进行更精准的查询。

  可实现数值类型字段的比较，格式为字段：值或字段 >= 值，通过and、or等进行组合。也可以和全文搜索组合使用，同样通过and、or组合。

  高防网站访问日志和攻击日志同样可以基于字段查询，各个字段的含义、类型、格式等信息请查看全量日志字段说明。

  示例：

  - 查询多字段

    搜索所有www.aliyun.com被CC攻击的日志：

    ```
    matched_host: www.aliyun.com and cc_blocks: 1
    ```

    如果要搜索某个客户端10.2.3.4对网站www.aliyun.com的所有错误404的访问日志，可以这样：

    ```
    real_client_ip: 10.2.3.4 and matched_host: www.aliyun.com and
    status: 404
    ```

     说明：

示例中用的字段matched_host、cc_blocks、real_client_ip和status等都是DDoS高防访问与攻击日志的字段，详细的字段列表和信息，可以参见全量日志字段说明。

- 查询数值字段

  搜索所有响应时间超过5秒的慢请求日志：

  ```
  request_time_msec > 5000
  ```

  也支持区间查询，查询响应时间大于5秒且小于等于10秒的日志：

  ```
  request_time_msec in (5000 10000]
  ```

  该查询还可以通过以下语句实现：

  ```
  request_time_msec > 5000 and request_time_msec <= 10000
  ```

- 查询日字是否存在

  针对特定字段是否存在进行查询：

  ■ 查询存在ua_browser字段的日志：ua_browser: *

  ■ 查询不存在ua_browser字段的日志：not ua_browser: *

详细的查询语法说明请参见索引与查询。

分析语法

您可以使用SQL/92语法对日志数据进行分析与统计，日志服务支持的语法与函数请查看#unique_65。

说明：

- 分析语句中可以省略SQL标准语法中的from 表格名语句，即from log。
- 日志数据默认返回前100条，您可以通过#unique_66修改返回范围。

基于日志时间的查询分析

每一条高防日志都有一个字段time表示日志的时间，格式为年-月-日T时:分:秒+时区。例如2018-05-31T20:11:58+08:00，其中时区为UTC+8区，也就是北京时间。同时，每条日志都有一个内置字段：__time__，也表示这条日志的时间，以便在统计时进行基于时间的计算。其格式为Unix时间戳，本质是一个自从1970-1-1 0:0:0 UTC时间开始的累计过去的秒数。因此实际使用时，经过可选的计算后，需要格式化才可以展示。

- **选择并展示时间**

  这里在特定时间范围内，选择网站`www.aliyun.com`被CC攻击的最新10条日志，展示其中时间、来源IP以及访问客户端，直接使用字段`time`：

```
matched_host: www.aliyun.com and cc_blocks: 1
|  select time, real_client_ip, http_user_agent
    order by time desc
    limit 10
```

  图 4-12: 选择并展示时间

- **计算时间**

  查询CC攻击过后的天数，可以使用`__time__`进行计算：

```
matched_host: www.aliyun.com  and cc_blocks: 1
|  select time,
          round((to_unixtime(now()) - __time__)/86400, 1) as "
days_passed",              real_client_ip, http_user_agent
      order by time desc
      limit 10
```

  说明：

  这里使用`round((to_unixtime(now()) - __time__)/86400, 1)`，先用`to_unixtime`将`now()`获取的时间转化为Unix时间戳，再与内置时间字段`__time__`相减，获得已经过去

的时间秒数。最后除以86400，即一天的总秒数，再用函数round(data, 1)圆整为小数点后1位数的值，可得出每条攻击日志距离现在已经过去了几天。

图 4-13: 查询结果

time	days_passed	real_client_ip	http_user_agent
2019-06-20T11:04:11+08:00	20.9		
2019-06-20T11:04:11+08:00	20.9		
2019-06-20T11:04:11+08:00	20.9		
2019-06-20T11:04:11+08:00	20.9		
2019-06-20T11:04:10+08:00	20.9		
2019-06-20T11:04:10+08:00	20.9		
2019-06-20T11:04:10+08:00	20.9		
2019-06-20T11:04:10+08:00	20.9		
2019-06-20T11:04:10+08:00	20.9		
2019-06-20T11:04:10+08:00	20.9		

- 基于特定时间分组统计

  如果想知道特定时间范围内，某个网站每天被CC攻击的趋势如何，使用如下SQL：

```
matched_host: www.aliyun.com  and cc_blocks: 1
| select date_trunc('day', __time__) as dt,
         count(1) as PV
      group by dt
      order by dt
```

说明：

这里使用内置时间字段__time__，传给函数date_trunc('day', ..)进行时间按天对齐，将每条日志分组到了其所属的天的分区中进行统计总数（count(1)），并按照分区时间块

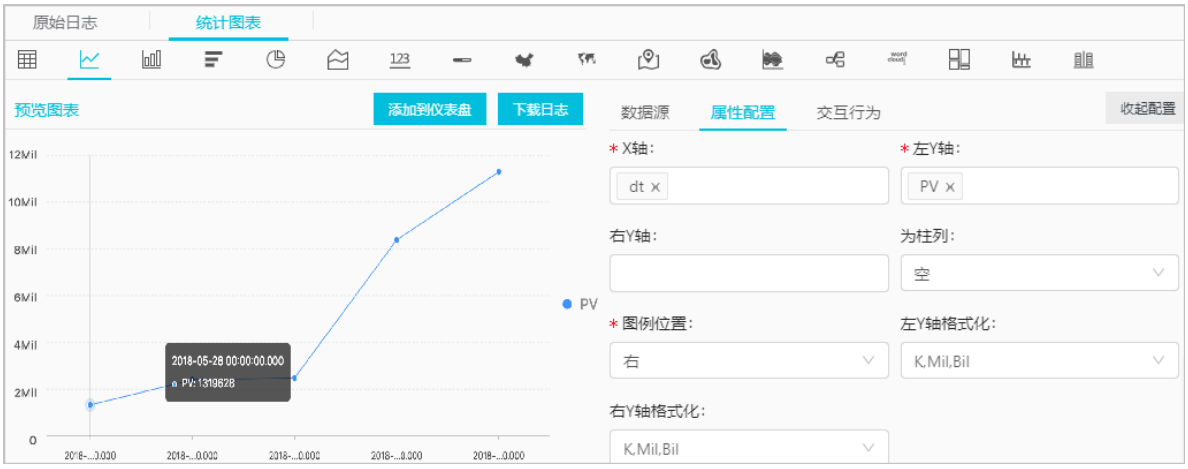
排序。函数date_trunc第一个参数提供更多其他单位进行对齐，包括second、miniute、hour、week、month、year等，函数说明请参见*#unique_67*。

图 4-14: 统计结果

dt	PV
2018-05-28 00:00:00.000	1319628
2018-05-29 00:00:00.000	2402020
2018-05-30 00:00:00.000	2473332
2018-05-31 00:00:00.000	8381076
2018-06-01 00:00:00.000	11293642

折线图方式展示：

图 4-15: 折线图



- **基于时间分组统计**

  如果想知道更灵活的分组下时间规律，例如某个网站每5分钟被CC攻击的趋势，需要进行数学计算。可以使用如下SQL：

```
matched_host: www.aliyun.com  and cc_blocks: 1
| select from_unixtime(__time__ - __time__% 300) as dt,
         count(1) as PV
      group by dt
      order by dt
```

```
        limit 1000
```

说明：

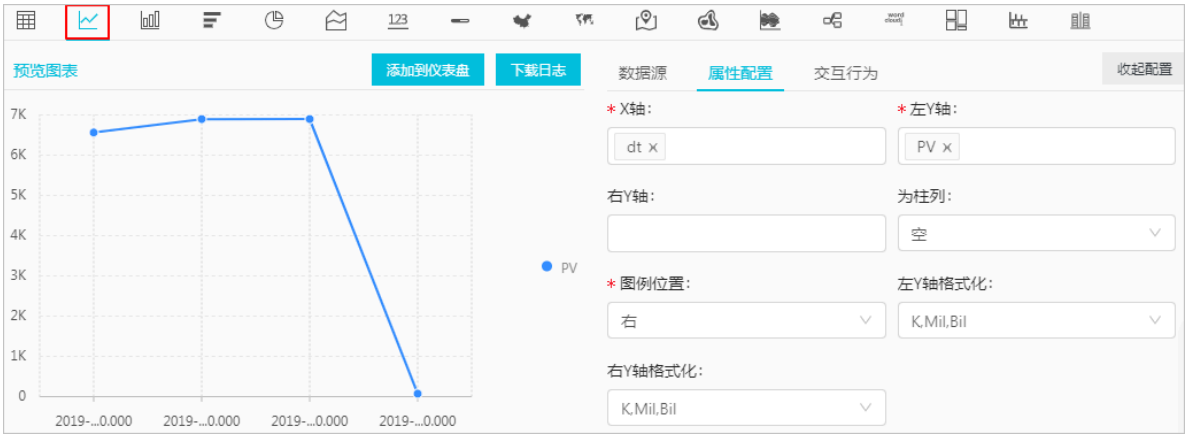
使用计算的内置时间字段计算`__time__ - __time__% 300`，同时使用函数`from_unixtime`进行格式化，将每条日志分组到了一个5分钟（300秒）的分区中进行统计总数（count(1)），并按照分区时间块排序，获得前1000条，相当于选择时间内的前83小时的数据。

图 4-16: 时间分组统计结果

dt	PV
2019-06-20 17:35:00.000	1430
2019-06-20 17:40:00.000	6893
2019-06-20 17:45:00.000	6902
2019-06-20 17:50:00.000	5230

折线图方式展示：

图 4-17: 折线图



更多关于时间解析的函数，例如将一个时间格式转化为另外一个格式，需要使用`date_parse`与`date_format`，函数说明请参见*#unique_67*。

基于客户端IP的查询分析

高防日志中有反映真实客户端IP的字段`real_client_ip`，但用户通过代理并跳转头中IP有误等情况下无法拿到用户真实IP时，可以直接使用直连客户端IP的字段`remote_addr`来代替。

- **攻击者国家分布**

  这里对某个网站进行CC攻击的来源国家分布：

```
matched_host: www.aliyun.com  and cc_blocks: 1
| 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
```

说明：

这里先用函数`if(condition, option1, option2)`来选择字段`remote_addr`或者`real_client_ip`（当`real_client_ip`为`-`时）。然后将获得的IP传给函数`ip_to_country`得到这个IP对应的国家信息。

图 4-18: 攻击者国家分布-分析结果

country	攻击次数
菲律宾	6321
斯洛文尼亚	521
吉布提	91
多哥	9
印度	14436
爱沙尼亚	65
莱索托	12

世界地图方式展示：

图 4-19: 世界地图

- **访问者省份分布**

  如果您希望获得更详细的基于省份的分布，可以使用函数`ip_to_province`，例如：

```
matched_host: www.aliyun.com  and cc_blocks: 1
| SELECT ip_to_province(if(real_client_ip='-', remote_addr,
real_client_ip)) as province,
         count(1) as "攻击次数"
         group by province
```

   **说明：**

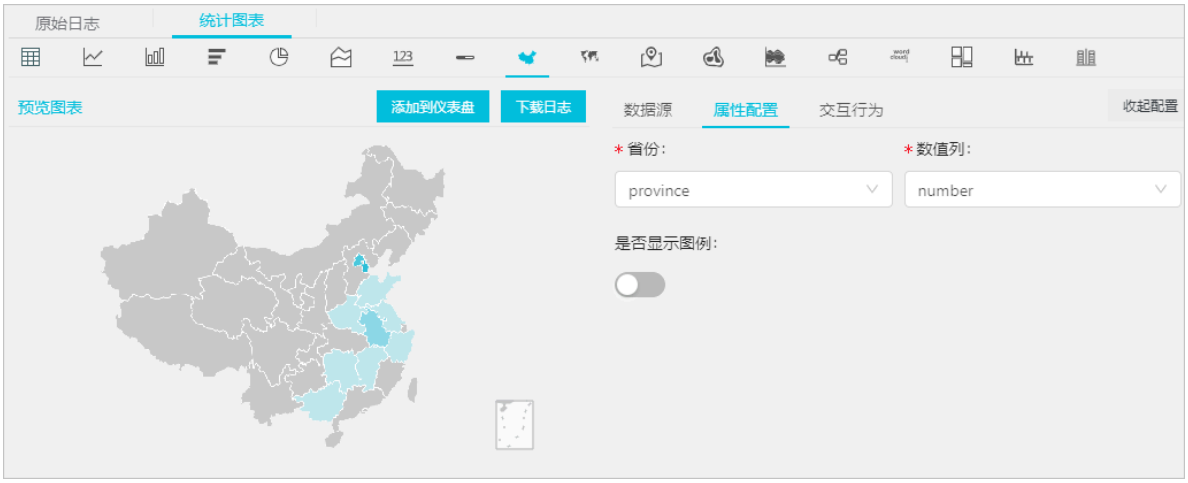
这里使用了另外一个IP函数`ip_to_province`来获得一个IP的所属省份。如果是中国以外的IP地址，依然会尝试转化为其国家所属省份（州），但在选择中国地图展示时，会无法展示出来。

图 4-20: 访问者省份分布-分析结果

province	攻击次数
江苏省	53
湖南省	2
北京市	509026
河南省	1411
安徽省	205629
广西壮族自治区	503
天津市	723121
浙江省	318

中国地图方式展示：

图 4-21: 中国地图



- **攻击者热力分布**

  如果期望获得一张攻击者的热力图，可以使用另外一个函数`ip_to_geo`，例如：

```
matched_host: www.aliyun.com  and cc_blocks: 1
| SELECT ip_to_geo(if(real_client_ip='-', remote_addr, real_clien
t_ip)) as geo,
```

```
        count(1) as "攻击次数"
        group by geo
        limit 10000
```

说明：

这里使用了另外一个IP函数ip_to_geo来获得一个IP的所在经纬度，并获取前1万条。

图 4-22: 攻击者热力分布-分析结果

geo	pv
31.8639,117.281	81378
36.6683,116.997	656
30.0135,120.288660	72
39.1422,117.177	723121
31.1461,118.571	124143
22.8167,108.316670	503
25.85,114.933	673
32.2109,119.455	53

高德地图方式展示：

图 4-23: 高德地图

基于IP的更多解析功能，例如获得IP所属运营商`ip_to_provider`**、判断IP是内网还是外网**`ip_to_domain`**等，可以参见***#unique_68*。