阿里云
DDoS基础防护

DDoS高防（国际）

文档版本：20190214

法律声明

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

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

通用约定

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

目录

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。

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。

：

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。

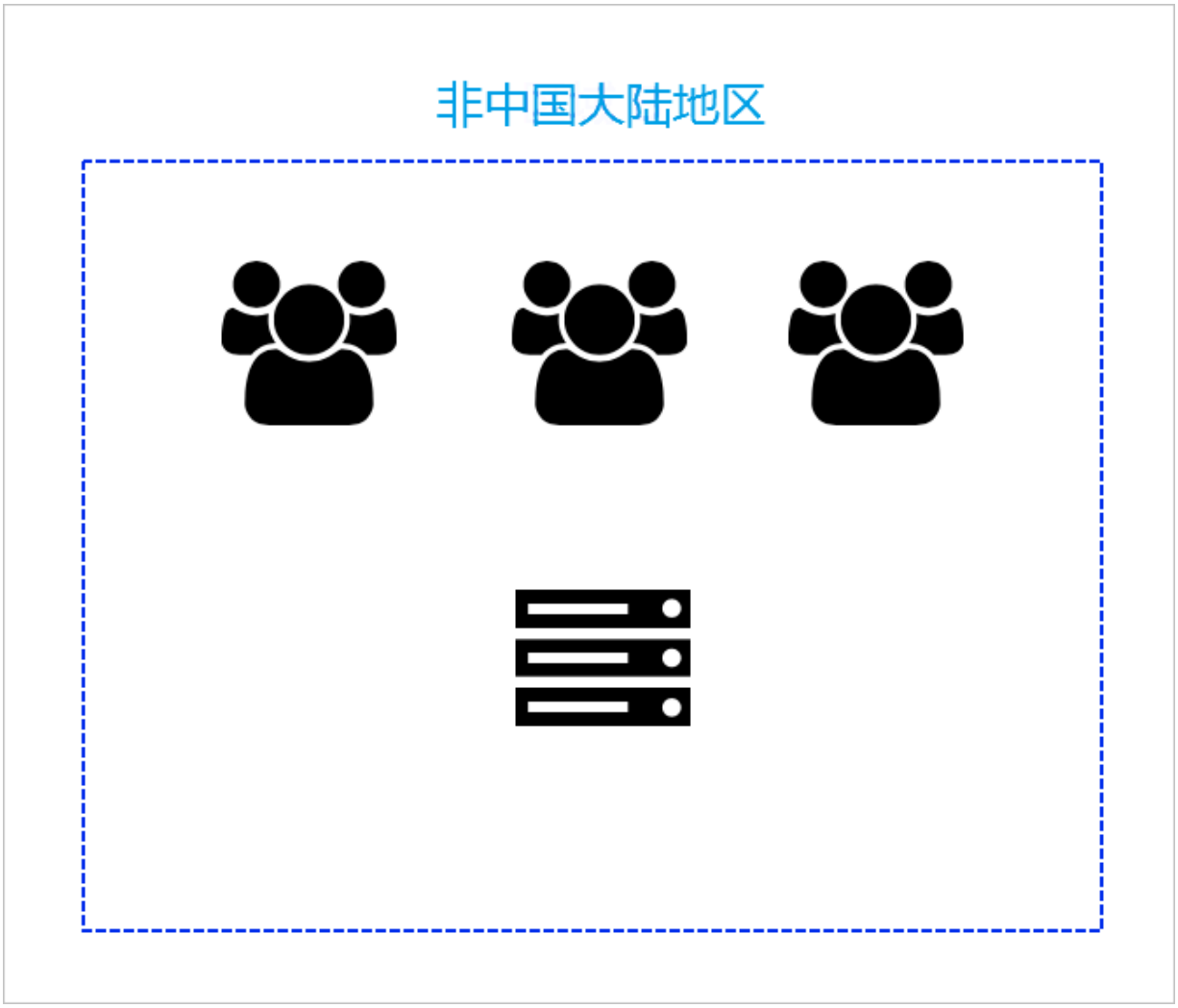
说明:

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。

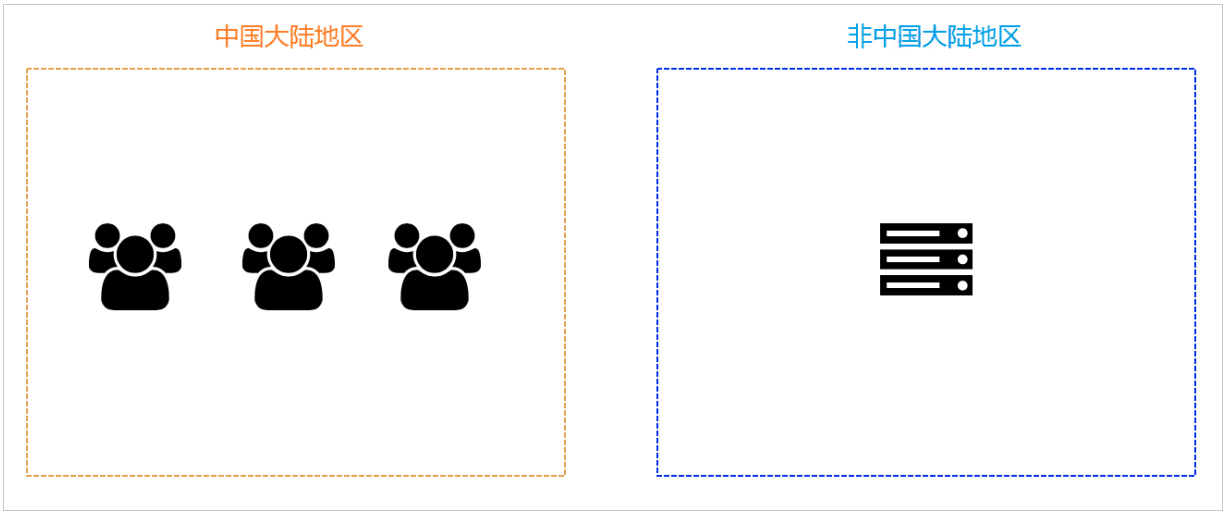
对于服务器部署在非中国大陆地区的业务，主要可分为以下三个场景：

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：

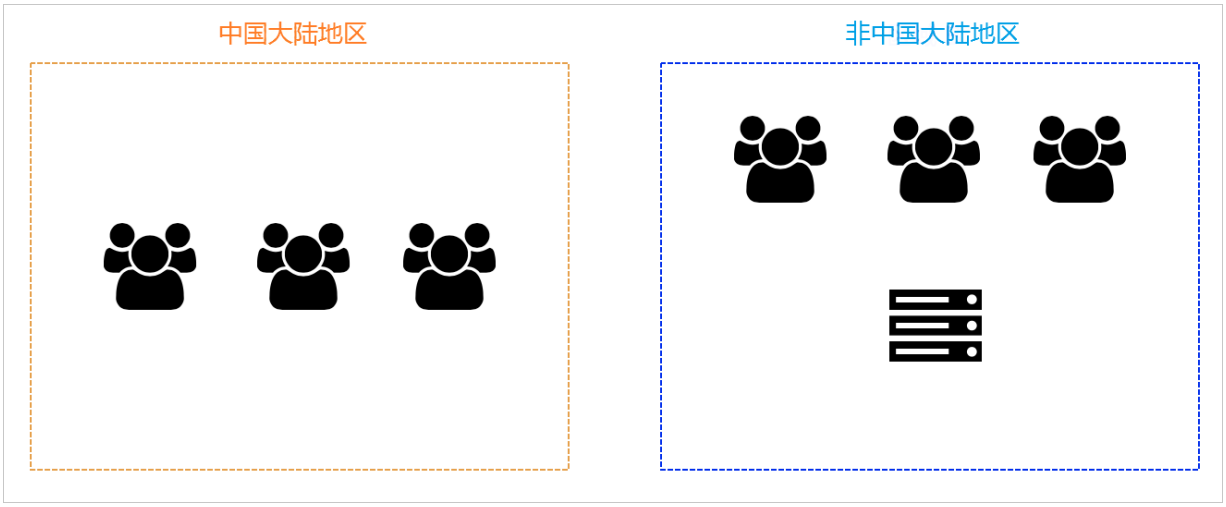
- 方案一

  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。

：
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。

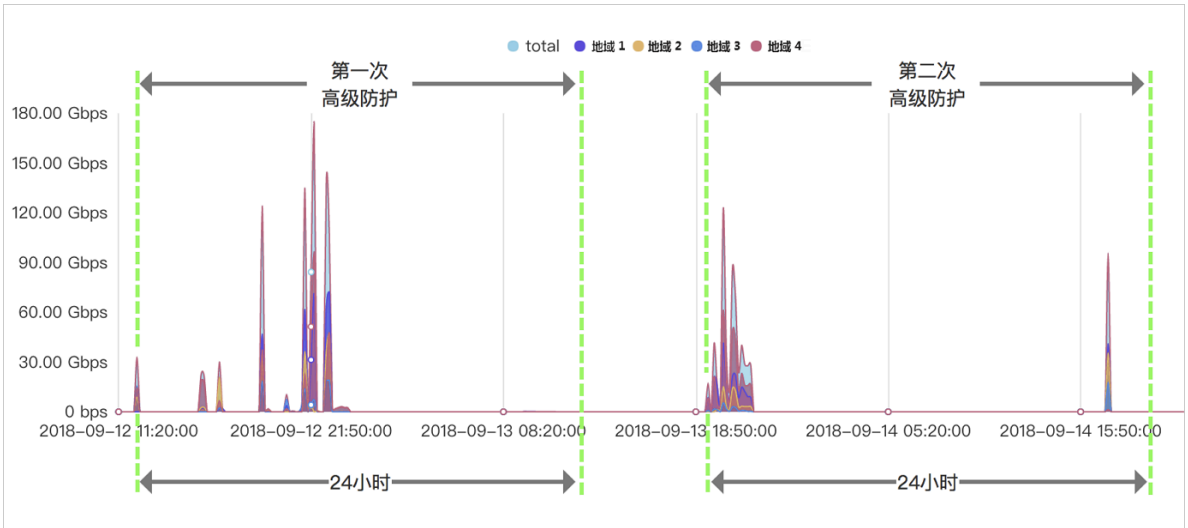
DDoS高防（国际）的套餐版本

- 保险版

  DDoS高防（国际）保险版每月赠送两次高级防护（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: 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。	每10个域名：1,000 元/月 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	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

更多信息

如何选择业务带宽规格

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和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:

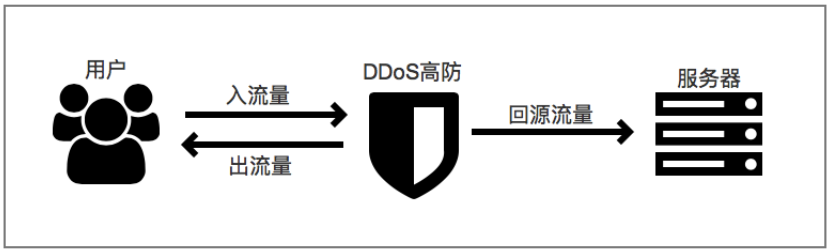
一般情况下，网络出方向的流量会比较大。

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。

防护域名规格说明

DDoS高防（国际）实例默认支持添加10个域名接入防护，包含一个一级域名和该一级域名的子域名或泛域名。

例如，默认情况下，您可以添加一个一级域名（`abc.com`）和最多九个该域名的子域名或泛域名（例如，`www.abc.com`，`\*.abc.com`，`mail.abc.com`，`user.pay.abc.com`，`x.y.z.abc.com`等）。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。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）实例扩展防护域名数量。

> **说明:**
> 每增加10个防护域名，可多添加一个一级域名。例如，您需要添加abc.com和xyz.com两个一级域名配置，则需要选择20个防护域名数的规格。

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）保险版实例默认赠送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，保险版实例默认赠送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赠送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	3年
购买单价	10,500 元/次

> **:**
> 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。	每月免费赠送两次
全局高级防护	云账号	三年	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
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。

同时，DDoS高防（国际）加速线路实例默认包含以下业务规格：

 说明:
加速线路实例的规格应与搭配使用的DDoS高防（国际）保险版或无忧版实例的业务规格配置保持一致。

业务规格	规格说明	默认情况
防护端口数	实例支持添加的TCP/UDP端口数量。	默认5个，请设置为与需要搭配使用的保险版或无忧版实例的防护端口数一致。
防护域名数	实例支持添加的HTTP/HTTPS域名数量。	默认10个，请设置为与需要搭配使用的保险版或无忧版实例的防护域名数一致。  说明: 每10个防护域名数包含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	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。	500 QPS

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。

背景信息

> **说明:**
> 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，参考非网站业务接入*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 > 网站接入页面，单击添加网站。
3. 在填写网站信息页面，填写需要防护的网站信息，单击添加。

参数	描述	说明
网站	需要防护的网站域名。	支持填写一级域名（如 test.com）或二级域名（如 www.test.com），且二者互不影响。同时，支持填写泛域名（如 .test.com），系统将自动匹配该泛域名的二级域名。
转发协议	该网站支持的协议类型。	如果您的网站支持HTTPS或Websockets加密认证，可勾选HTTPS或Websockets协议并在添加网站配置后上传对应的证书和私钥。

参数	描述	说明
服务器地址	该网站域名的源站服务器地址。	网站接入DDoS高防（国际）实例进行防护后，DDoS高防会将过滤后的访问流量转发至该服务器地址。 · （推荐）勾选源站IP，填写源站服务器的IP（如云服务器ECS实例的IP、负载均衡SLB实例的IP等），配置成功后高防将流量转发至该源站IP。 说明: 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IP Hash方式进行轮询实现负载均衡。 · 勾选源站域名，填写服务器回源域名（如对象存储OSS的CNAME等），配置成功后高防将流量转发至该域名。 说明: 服务器回源域名不应与所防护的网站域名相同。
服务器端口	该网站域名的源站端口。网站接入DDoS高防（国际）实例进行防护后，DDoS高防会将过滤后的访问流量转发至该端口。	· HTTP和Websocket协议默认为80端口。 · HTTPS和Websockets协议默认为443端口。
选择高防独享IP	防护该网站域名的DDoS高防（国际）实例。	一个网站域名最多支持配置8个DDoS高防（国际）实例独享IP。

4. 在该网站的域名解析服务提供商处，修改该网站域名的DNS解析记录。

   将域名解析至所选择的DDoS高防（国际）实例的独享IP，将网站业务流量切换至DDoS高防（国际）实例。

   说明:
   如果您希望在正式切换业务流量前，在本地测试已配置的DDoS高防（国际）的转发规则是否生效，您可以单击返回网站列表。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，选择实例列表，找到防护该网站域名的DDoS高防（国际）实例，记录该实例所对应的独享IP。

b) 前往您网站域名的DNS服务提供商处，修改DNS解析，将该网站域名解析的A记录指向DDoS高防（国际）实例的独享IP。

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

c) 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。

5. （可选）配置源站保护，具体操作参考高防源站保护。

> 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

：

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）。

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。

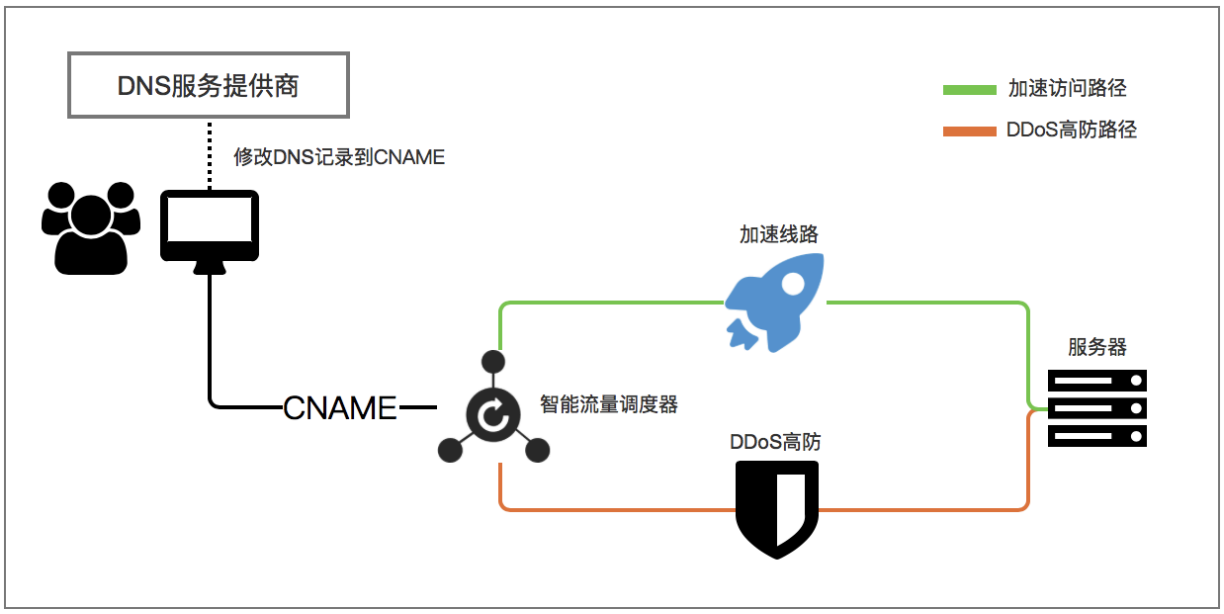
3.4 配置DDoS高防（国际）加速线路

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，查看*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。

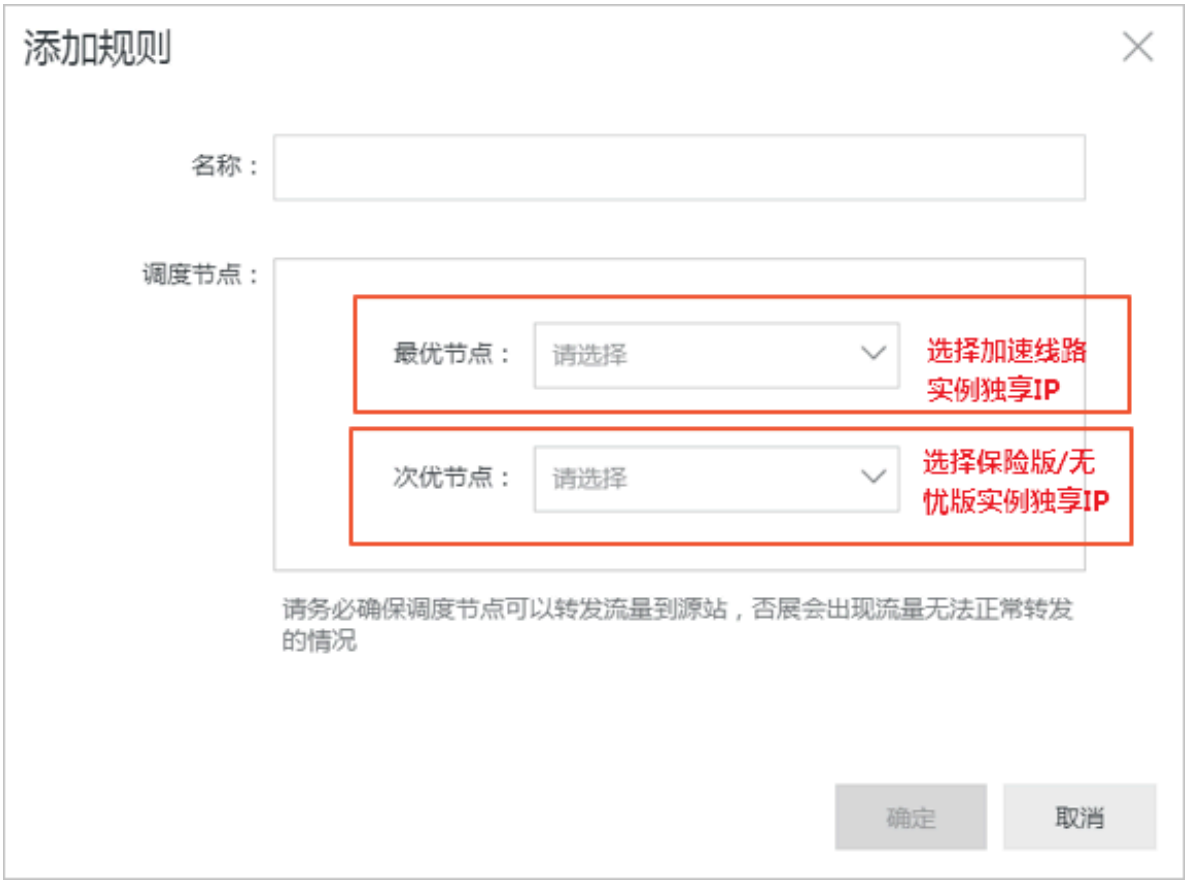
   说明：
   您只需完成网站或非网站业务接入配置，无需修改DNS解析。

   - 网站域名接入DDoS高防（国际）：参考网站业务接入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：参考非网站业务接入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. 完成网站域名或业务端口接入配置后，在接入配置 > 安全流量调度器页面，单击添加规则。

4. 在添加规则对话框中，设置规则条件，单击确定。



- 最优节点：设置为DDoS高防（国际）加速线路实例的独享IP。
- 次优节点：设置为DDoS高防（国际）保险版/无忧版实例的独享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，安全流量调度器将自动将流量切换至防护线路进行流量清洗。

安全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。

3.5 业务配置批量导入导出

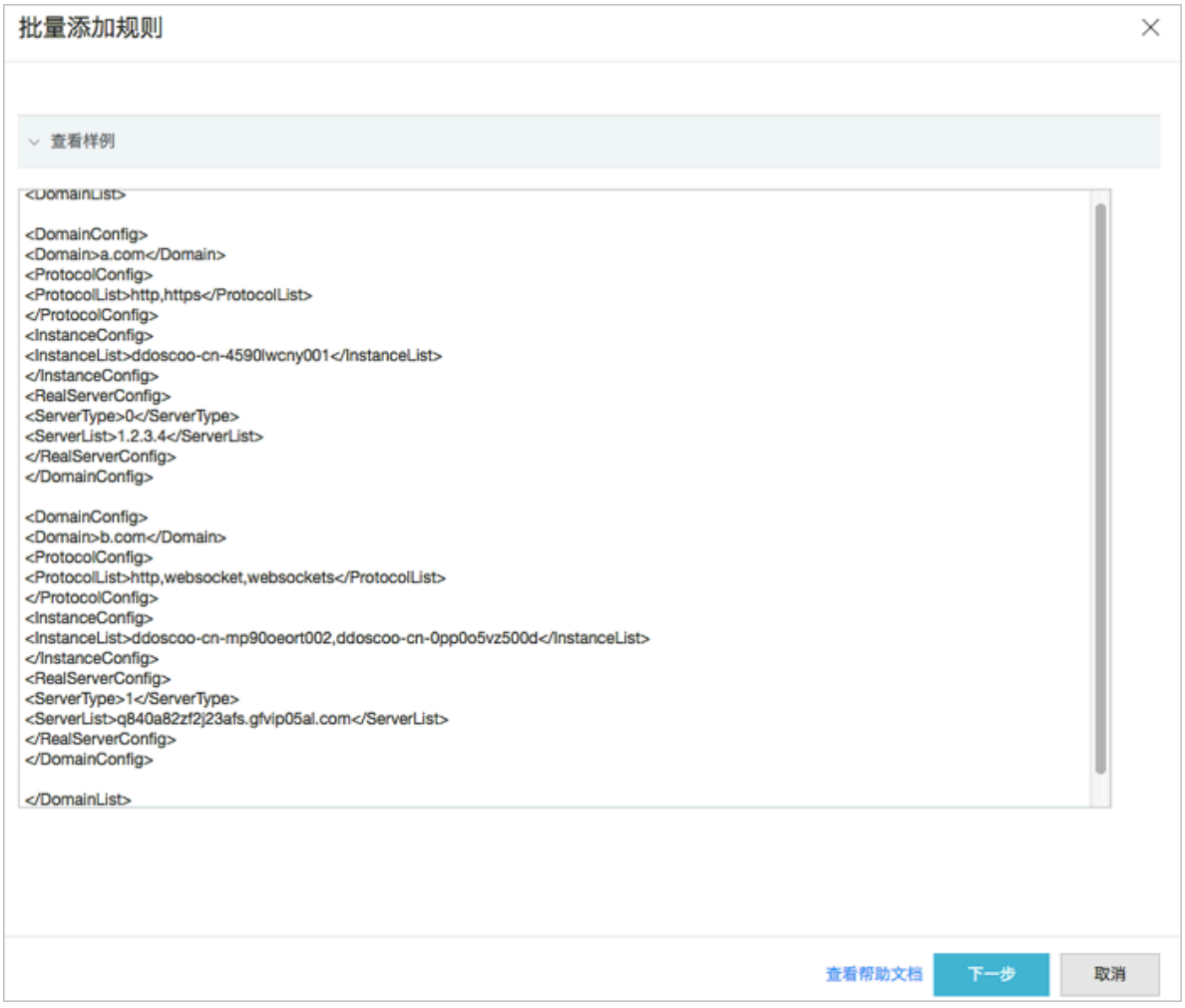
当您的网站域名配置或四层转发规则配置数量过多时，如果您需要保存当前时间点的业务接入配置或进行配置迁移，您可以通过业务配置的批量导入/导出功能，快速完成这类操作。

- 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
```

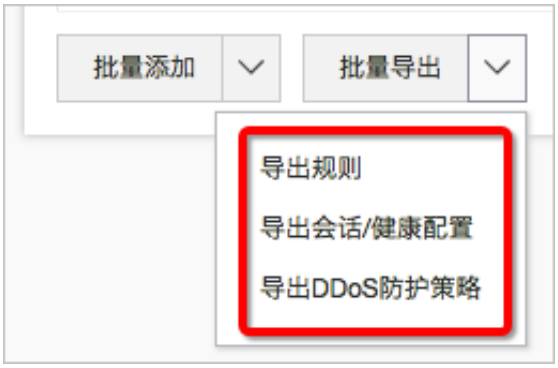
字段含义从左至右以此为转发协议端口、转发协议、源新建连接限速、源并发连接限速、目的新建连接限速、目的并发连接限速、包长度最小值、包长度最大值、虚假源与空连接(仅TCP协议时生效，空连接开启前需要先开启虚假源)。

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。