阿里云
DDoS高防IP

DDoS基础防护服务

文档版本：20190902

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基础防护

阿里云免费为用户提供最高5G的默认DDoS防护能力。在此基础上，阿里云推出了安全信誉防护联盟，将基于安全信誉分进一步提升DDoS防护能力，用户最高可获得100G以上的免费DDoS防护流量。

DDoS基础防护具备以下特性：

- 安全信誉防护联盟服务

  在已有基础DDoS防护上，提供无偿安全信誉防护服务，基于信誉享受增量防护能力。
- 覆盖常见DDoS防护类型

  包括但不限于以下攻击类型：ICMP Flood、UDP Flood、TCP Flood、SYN Flood、ACK Flood。
- 提升攻击防御阈值

  根据安全信誉，动态提升防护阈值。
- 缩短黑洞时长

  根据安全信誉，缩短极端攻击下黑洞默认时长，使您的业务更快速恢复。
- 开放信誉组成

  联盟用户可根据信誉组成建议自行维护信誉，获得更多的防护能力。

更多信息，请参见DDoS基础防护产品详情页。

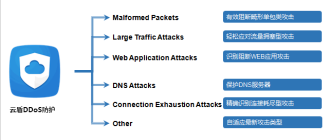
1.2 产品架构

目前，DDoS基础防护在引流技术上支持BGP与DNS两种方案。防护采用被动清洗方式为主、主动压制为辅的方式。对DDoS攻击进行综合运营托管，可让您在攻击下高枕无忧。

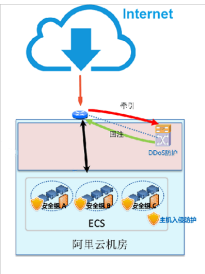
针对DDoS攻击在传统的代理、探测、反弹、认证、黑白名单、报文合规等标准技术的基础上，并结合Web安全过滤、信誉、七层应用分析、用户行为分析、特征学习、防护对抗等多种技术，对攻击威胁进行阻断过滤，保证被防护用户在攻击持续状态下，仍可对外提供业务服务。

当前，阿里云建设的DDoS防护系统，防护量级达到T级。同时，阿里云不断在各地扩容防护能力节点。

DDoS基础防护服务基于阿里云自主研发的云盾产品，帮助您防御SYN Flood、UDP Flood、ACK Flood、ICMP Flood、DNS Query Flood、NTP reply Flood、CC攻击等三层到七层DDoS攻击。DDoS基础防护服务支持防御的攻击类型如下图所示。



DDoS基础防护主要采用在阿里云机房出口处建设DDoS攻击检测及清洗系统，采用旁路部署方式。 DDoS基础防护网络拓扑架构如下图所示。



1.3 功能特性

云盾DDoS基础防护服务提供以下功能。

功能	子功能	特性描述
攻击防护	畸形报文过滤	过滤Frag flood，Smurf，Stream flood， Land flood攻击。
攻击防护	畸形报文过滤	过滤IP畸形包、TCP畸形包、UDP畸形包。
攻击防护	传输层DDoS攻击防护	过滤SYN flood， ACK flood， UDP flood， ICMP flood、RST flood攻击。
攻击管理	攻击证据收集	自动进行异常流量抓包。
攻击管理	攻击事件管理	支持对攻击事件、攻击流量的管理统计。

1.4 产品优势

云盾DDoS基础防护服务具有以下功能优势。

优质的防护线路

- 受到DDoS攻击不会影响访问速度。

- 带宽充足，不会被其他用户连带影响。
- 优质带宽保证业务可用和稳定。

精准防护

- 精准识别攻击，秒级开启防护。
- 自研清洗设备和算法，保证极低误杀。
- 单点多点清洗不会相互影响。

免安装免维护

- 无需采购昂贵清洗设备。
- 自动为云上客户开通，免安装。
- 智能业务学习和配置防护规则。

免费

- 基础DDoS防护免费。
- 阿里云用户免费加入安全信誉防护联盟。

1.5 应用场景

DDoS基础防护适用于互联网DDoS攻击防护。

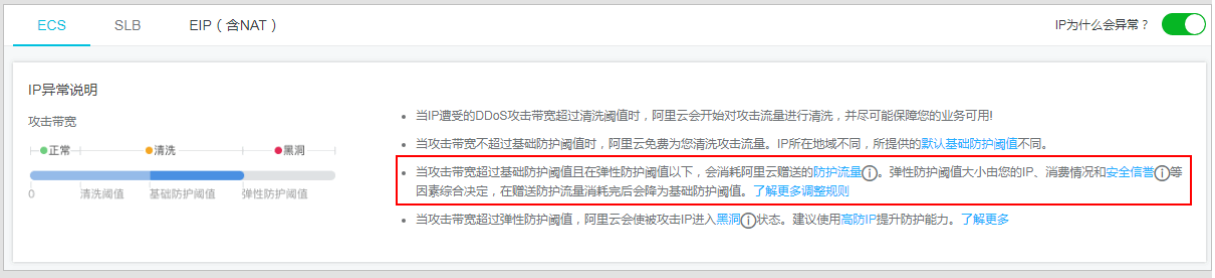
适用范围：阿里云ECS、SLB、EIP、NAT、WAF等云产品的免费防护。

应用限制：不超过5G的DDoS攻击防护场景。

1.6 安全信誉防护联盟

说明:

自2018年7月31日起，默认所有阿里云用户自动加入安全信誉防护联盟。您可以登录DDoS基础防护控制台查看详情。



一、什么是安全信誉防护联盟

为了给您带来更好的安全防护体验，并且提升安全防护能力，阿里云开展安全信誉防护联盟计划。加入该计划后，依据安全信誉评估结果，可获得阿里云提供的动态的DDoS攻击防护能力。

目前，安全信誉防护联盟全量开放，加入联盟计划您不需要支付任何费用。

二、安全信誉联盟的优势

- 提升攻击防护阈值。根据安全信誉动态调整防护阈值，绝大部分用户的防护阈值不小于机房默认黑洞触发阈值，使您的业务被攻击打进黑洞的几率降低。
- 开放信誉组成。联盟用户可根据信誉组成建议实施优化，获得更多的防护能力。

三、联盟计划下安全防护的工作机制

- 根据评分值动态计算用户的DDoS防护能力，绝大部分用户都将免费获得增量DDoS防护量。
- 根据安全信誉分计算出的黑洞触发阈值（即攻击防护上限，超过该上限就触发黑洞策略），可用于ECS及SLB当天低于该阈值攻击的无偿防护。如果攻击大小超过安全信誉计算的最新阈值，则会触发黑洞，黑洞触发阈值也会下降到原默认阈值。
- 随着攻击的发生，将影响下个周期的安全信誉评分。
- 加入联盟计划所获得的安全防护能力，是一个共享资源池，阿里云将尽力提供给您根据您的信誉评分而获得的安全防护带宽。但在加入联盟的会员遭遇集体性的攻击或其他等恶意攻击事件，导致共享资源池的资源耗尽时，阿里云将会降低给您的安全防护带宽。
- 针对个别黑洞过于频繁的用户，阿里云保留延长黑洞时长和降低黑洞阈值的权利，具体黑洞阈值和黑洞时长以控制台显示为准。
- 如攻击流量超过您的安全信誉防护联盟提供的增量防护能力，您应及时按云盾的防护建议购买DDoS高防产品，以获得更好的安全防护能力，否则您的ECS、SLB可能会被攻击导致服务中断。
- 请注意信息安全，保密自有安全信誉分及据此得出的相关信息。

四、安全信息防护联盟服务条款

1 您理解并确认，您不应利用基于加入联盟计划而将阿里云提供给您的安全防护能力从事如下行为：

1.1 为他人提供有偿或无偿安全防护的业务；

1.2 进行任何非法业务、进行任何不符合阿里云在阿里云官网（www.aliyun.com）公布的使用目的或流程的行为、或进行任何经阿里云自身判断不符合安全防护能力使用目的行为；

1.3 进行上传、下载或传播如下信息的行为或为他人上传、下载或传播该等信息提供便利：

1.3.1 违反国家规定的政治宣传和/或新闻；

1.3.2 涉及国家秘密和/或安全；

1.3.3 封建迷信和/或淫秽、色情和/或教唆犯罪；

1.3.4 博彩有奖、赌博游戏、“私服”、“外挂”等非法互联网出版活动；

1.3.5 违反国家民族和宗教政策；

1.3.6 妨碍互联网运行安全；

1.3.7 侵害他人合法权益和/或其他有损于社会秩序、社会治安、公共道德的活动；

1.3.8 其他违反法律法规、部门规章或国家政策的内容。

1.4 修改、翻译、改编、出租、转许可、在信息网络上传播或转让阿里云提供的软件/服务，也不得逆向工程、反编译或试图以其他方式发现阿里云提供的软件的源代码；

1.5 进行任何破坏或试图破坏网络安全的行为（包括但不限于钓鱼，黑客，网络诈骗，网站或空间中含有或涉嫌散播：病毒、木马、恶意代码，及通过虚拟服务器对其他网站、服务器进行涉嫌攻击行为如扫描、嗅探、ARP欺骗、DDoS等）；

1.6 不进行任何改变或试图改变阿里云提供的系统配置或破坏系统安全的行为；

1.7 不利用阿里云提供的服务/能力从事损害阿里云、阿里云的关联公司或阿里巴巴集团内包括但不限于阿里巴巴、淘宝、支付宝、阿里妈妈、阿里金融等（以下统称为阿里巴巴公司）各公司、网站合法权益之行为，前述损害阿里巴巴公司、网站合法权益的行为包括但不限于违反阿里巴巴公司公布的任何服务协议/条款、管理规范、交易规则等规范内容、破坏或试图破坏阿里巴巴公司公平交易环境或正常交易秩序等；

1.8 不从事其他违法、违规或违反本《安全信息防护联盟规则》的行为；

1.9 您理解阿里云同意您加入计划的前提，是基于您做出的前述承诺，如您违反您的前述承诺，阿里云有权终止向您提供基于本联盟而提供的服务/能力，同时有权经通知您，终止您的联盟会员身份。

2 您理解并确认，阿里云有权根据自身的业务计划或联盟运营情况等因素，随时终止本联盟计划而不负任何责任，在计划终止前，阿里云将提前通知您。计划终止时，您基于加入联盟计划而获得的能力/服务将一并终止。

3 您理解并确认，您已阅读《联盟计划下安全防护的工作机制》以及本《安全信誉联盟规则》并知悉您加入该计划后将会产生的结果，您加入该计划是出于您的自愿以及经过独立审慎的判断，因此，您对自己加入本联盟的行为及其产生的结果负责。

4 阿里云和您都应对您是否加入该联盟计划的情况进行保密，除非该信息已进入共有领域或阿里云依据双方的另行约定、法律法规的规定、以及相关权力机关的要求、命令、判决披露。同时您需

对您安全信誉分及在此基础上生成的黑洞触发阈值及相关安全信誉信息保密，以防止该信息泄露后，引起黑客针对性攻击等不利后果的发生。

5 阿里云可能会定期或不定期的对于联盟计划下的安全防护机制进行优化或变更，阿里云将经提前通知您后向您提供最新版本的服务/或依据最新的工作体制向您提供服务/能力，如您不同意经优化后的安全防护机制，你可申请退出联盟计划并终止使用阿里云向您提供的服务。

6 您理解并确认，您加入联盟计划所获得的安全防护能力，是联盟成员共享资源池，阿里云将尽力提供给您根据您的信誉评分而获得的安全防护带宽，但在联盟会员遭遇集体性的攻击或其他等恶意攻击事件，共享资源池的带宽资源耗尽时，阿里云将会降低给您的安全防护带宽但（应不低于原机房默认阈值）。

7 免责与责任限制：您加入联盟后，获得的阿里云提供的安全防护是阿里云采取的一种技术措施，您理解并确认，阿里云按照《安全信誉防护联盟计划》执行上述技术措施，即视为提供了无瑕疵的安全防护，在阿里云无故意或重大过失的情况下，阿里云不对安全防护的结果承担责任。

8 如因您的网站遭遇计算机病毒、网络入侵和攻击破坏（包括但不限于DDoS）等危害网络安全事项或行为（以下统称该等行为），如果超过服务说明中防护范围，将会造成网站或服务在一定时间内不可被最终用户访问（以下统称“服务不可用”）。您理解并确认，该类服务不可用为阿里云履行安全防护服务的正常履行行为，并将不视为阿里云对相关服务的违约；如该行为给阿里云带来危害，或影响阿里云与国际互联网或者阿里云与特定网络、服务器及阿里云内部的通畅联系，阿里云将保留暂停或终止按照联盟工作机制向您提供安全防护服务的权利（但阿里云暂停或终止时，将及时通知您），而无须承担任何义务和责任。

9 阿里云官网上公布的相关规则、规范和流程是本规则的完整组成部分，阿里云有权利随时对上述规则、规范和流程予以修改，并有权利在通知您后要求您符合最新修订的内容。

2 快速入门

2.1 快速入门

云盾DDoS基础防护默认开启，免费为您阿里云账号下的ECS、SLB和EIP实例提供不大于5G的DDoS攻击防护能力。

背景信息

使用DDoS基础防护时，您需要关注以下操作：

- 设置清洗阈值。当IP遭受的DDoS攻击带宽超过清洗阈值时，阿里云会开始对攻击流量进行清洗，并尽可能保障您的业务可用。
- 关注防护阈值。防护阈值分为基础防护阈值和弹性防护阈值。
  - 当攻击带宽不超过基础防护阈值时，阿里云免费为您清洗攻击流量。IP所在地域不同，所提供的默认基础防护阈值不同。
  - 当攻击带宽超过基础防护阈值且在弹性防护阈值以下，会消耗阿里云赠送的防护流量。弹性防护阈值大小由您的IP、消费情况和安全信誉等因素综合决定，在赠送防护流量消耗完后会降为基础防护阈值。了解更多调整规则。

操作步骤

1. 登录云盾DDoS基础防护管理控制台。
2. 选择地域。
3. 在基础防护 > 实例页面，选择要操作的实例类型：ECS、SLB、EIP（含NAT）。

4. 在实例列表中，选择要操作的实例。

- 单击实例IP，查看近7天内的流量和报文记录，以及DDoS攻击事件记录。

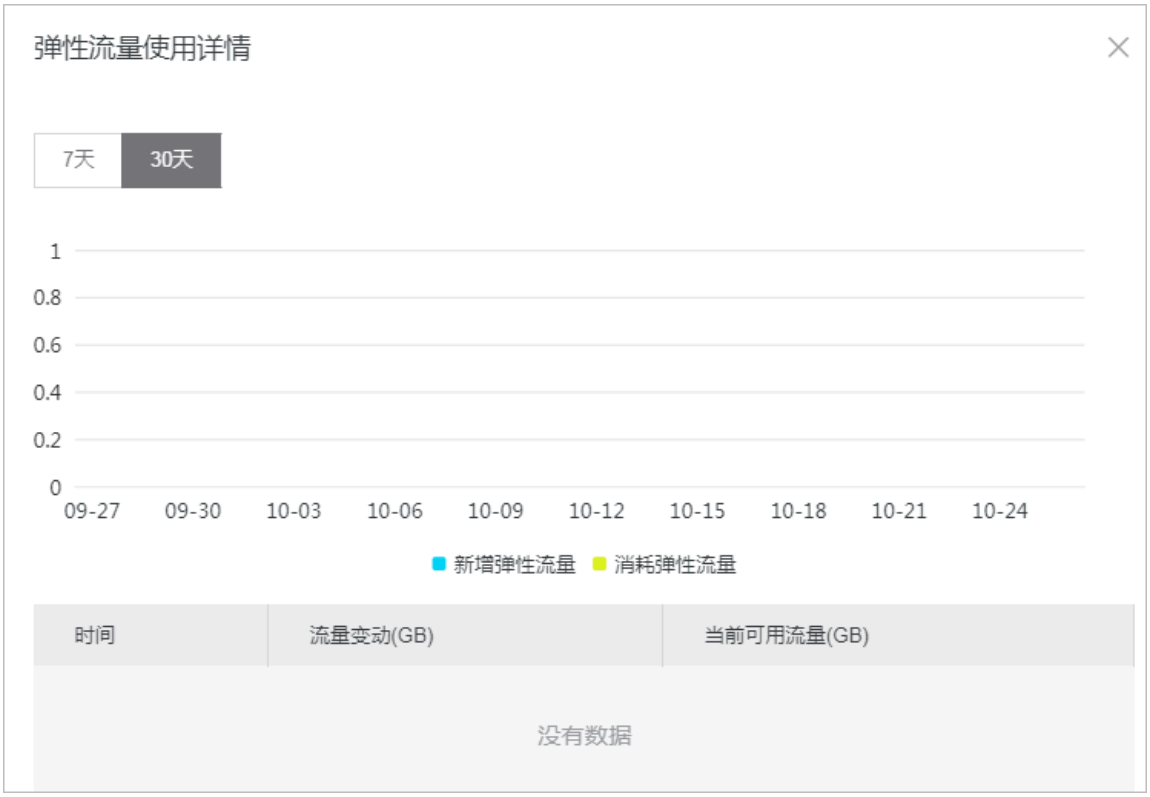
- 在实例详情对话框，单击清洗设置，可以选择手动设置或采用系统默认的清洗阈值。

5. 查看DDoS攻击防护说明。开启页面右上方DDoS攻击防护说明开关，可以查看以下信息：

- 查看当前可用防护流量。

说明:

单击防护流量，查看最近30日弹性流量的增加和消耗记录。



- **查看当前安全信誉分。**

说明:

单击安全信誉，查看安全信誉详情。

安全信誉分越高，您将获得更多的免费防护带宽加成。建议您参考安全信誉组成，维护安全信誉，获得更大的防护能力。

- **查看当前解除黑洞时间。**

说明:

单击黑洞，可查看阿里云黑洞策略详细说明。

3 用户指南

3.1 设置清洗阈值

云盾DDoS基础防护可以防御SYN Flood、UDP Flood、ACK Flood、ICMP Flood、DNS Flood等DDoS攻击。本文介绍了设置DDoS基础防护清洗阈值的方法。

操作步骤

1. 登录云盾DDoS基础防护管理控制台。
2. 选择地域。
3. 在基础防护 > 实例页面，选择要操作的云产品类型：ECS、SLB、EIP（含NAT）。
4. 在实例列表定位到需要操作的实例。

> **说明:**
> 您也可以通过实例ID、实例名称或实例IP搜索目标实例。

5. 单击实例IP，打开实例详情对话框，单击清洗设置。

6. 在清洗设置对话框中设置目标实例的清洗阈值，支持系统默认和手动设置。

- 选择系统默认，系统会根据云服务器的流量负载动态调整清洗阈值。
- 选择手动设置，可以手动选择流量和报文数量的清洗阈值。当超过此阈值后云盾便会开启流量清洗。

> 说明:
> - 清洗阈值需要设置成略高于实际访问值。阈值设置过高，起不到防御效果；而设置过低，DDoS基础防护触发流量清洗可能会影响正常的访问。
> - 当网站请求达到设置的清洗阈值时，DDoS基础防护触发流量清洗。如果清洗影响了正常的请求，请适当调高清洗阈值。
> - 建议在您的网站做推广或者活动时适当调大清洗阈值。

3.2 取消流量清洗

阿里云服务器默认提供DDoS攻击防御功能。当服务器遭受流量攻击时，监控系统自动检测到攻击，并为服务器清洗异常流量。

背景信息

清洗是指对进入服务器的数据流量进行实时监控，及时发现包括DDoS攻击在内的异常流量。在不影响正常业务的前提下，清洗掉异常流量，将可疑流量从原始网络路径中重定向到净化产品上进行恶意流量的识别和剥离，还原出的合法流量回注到原网络中转发给目标系统。

对于处于异常状态（清洗中）的IP，您可以手动取消清洗。

> 说明:
> 一个账号一天之内可以手动取消流量清洗三次。

操作步骤

1. 登录云盾DDoS基础防护管理控制台。

2. 选择地域。
3. 选择要操作的云产品，找到您想要取消的正在清洗中的IP，单击实例IP，打开实例详情对话框。

4. 在DDoS事件列表中，选择在清洗状态中的事件，单击取消清洗。

> **说明:**
> 单击证据下载，您可以下载针对该攻击事件的抓包文件作为证据供您向网监报案。

3.3 查看黑洞时长

服务器遭受DDoS攻击，触发黑洞后会根据该实例的安全信誉等级对被黑洞的服务器公网IP实行一定时间的访问限制。

背景信息

默认的黑洞时长是2.5小时，黑洞期间不支持解封。实际黑洞时长视攻击情况而定，从 30 分钟到 24 小时不等。 黑洞时长主要受以下因素影响：

- 攻击是否持续。如果攻击一直持续，黑洞时间会延长。
- 攻击是否频繁。如果用户首次被攻击，黑洞时间会自动缩短；反之，频繁被攻击的用户被持续攻击的概率较大，因此黑洞时间会自动延长。

具体黑洞阈值和实际黑洞时长以云盾DDoS基础防护控制台显示为准。

说明:

- 针对个别黑洞过于频繁的用户，阿里云保留延长黑洞时长和降低黑洞阈值的权利。
- 黑洞是网络运营商为阿里云提供的服务，运营商有明确的黑洞解除时间限制。因此，一般情况下黑洞时长不小于30分钟，且您账号的黑洞时长将根据您账号的安全信誉等级自动调整。

操作步骤

1. 登录云盾DDoS基础防护管理控制台。
2. 在基础防护 > 实例页面，开启右上角的DDoS攻击防护说明开关。
3. 查看当前的解除黑洞时长。

3.4 查看云盾安全信誉分计算依据

您可以在云盾DDoS基础防护控制台中查看您账号当前的安全信誉分、安全信誉详情和评分依据。

操作步骤

1. 登录云盾DDoS基础防护管理控制台。
2. 在基础防护 > 实例页面，开启右上角的DDoS攻击防护说明开关。
3. 查看当前的安全信誉分。

4. 单击安全信誉，查看安全信誉详情及评分依据。

说明:

建议您根据安全信誉评分标准维护您的安全信誉分，获取更多免费加成的DDoS防护能力。

3.5 设置黑洞告警通知

阿里云的DDoS黑洞通知提供告警通知功能。当您账号中的服务器遭受大量DDoS攻击触发黑洞时，您所设定的消息接收人将收到通知。

设置云盾安全信息通知的消息接收人

云盾安全信息通知支持以站内信、邮箱、短信的形式向您设置的消息接收人发送安全信息通知。

1. 登录消息中心管理控制台。
2. 在左侧导航栏，单击消息接收管理 > 基本接收管理。
3. 定位到云盾安全信息通知，单击账号联系人下的修改。

4. 在修改消息接收人对话框中，修改云盾安全信息通知的消息接收人。

> **说明:**
> 您也可以单击新增消息接收人，添加消息接收人。

3.6 查看IP进入黑洞的时间和原因

当ECS或SLB实例的公网IP遭到大量DDoS攻击，且DDoS攻击的流量超出对应的黑洞阈值后，该公网IP将被黑洞，所有来自外部的流量都将被丢弃，导致相关的业务无法正常访问。

背景信息

> **说明:**
> 各个地域实例的黑洞阈值可能不同。关于黑洞的具体说明，请参见阿里云黑洞策略。

您可以在云盾DDoS基础防护控制台中，查看IP进入黑洞的时间及所遭受的攻击流量。

操作步骤

1. 登录云盾DDoS基础防护管理控制台。
2. 选择地域。
3. 在基础防护 > 实例页面，选择要操作的实例类型：ECS、SLB、EIP（含NAT）。
4. 在实例列表定位到要操作的实例，被黑洞的实例的状态将显示为黑洞中。

> **说明:**

您可以通过实例ID、实例名称或实例IP搜索目标实例。

5. 单击实例IP，查看该实例的进入黑洞的时间和当时所遭受的攻击流量。

3.7 连接已被黑洞的服务器

本文介绍了在服务器进入黑洞时，通过阿里云同地域ECS服务器连接被黑洞服务器的方法。

背景信息

假如您的服务器遭受大流量攻击而进入黑洞，则所有来自外部的流量都会被丢弃，但是阿里云内部与该服务器同地域的云产品仍然能够正常连通该服务器。

因此，在您的服务器进入黑洞后，您可以使用阿里云内部的ECS云服务器连接该服务器。

操作步骤

1. 登录与被黑洞服务器同地域且可正常访问的ECS云服务器。

   说明:
   该ECS云服务器需要与被黑洞的服务器可连通，属于同一个专有网络VPC环境，且连接不被安全组的相关访问控制规则所阻断。更多信息，请参见#unique_23。

2. 在ECS云服务器中，通过工具或命令连接黑洞状态的服务器。
   通过ECS云服务器成功连接该服务器后，您可以将处于黑洞状态的服务器上的文件转移至已登录的ECS云服务器，您也可以通过这种方式变更该服务器上的配置文件等。

3.8 DDoS基础防护黑洞阈值

云盾DDoS基础防护各个地域默认初始黑洞触发阈值如下表所示（单位：bps）。

说明:

- 此黑洞默认阈值适用于阿里云ECS、SLB、WAF、EIP实例。
- 您的ECS、SLB、WAF、EIP实例的实际黑洞阈值还与您所购买的实例规格及带宽有关，以云盾管理控制台实际显示为准。更多详情，请参见如何查看实际黑洞阈值。

地区	1 核 CPU 规格 ECS 实例	2 核 CPU 规格 ECS 实例	4 核以上 CPU 规格 ECS 实例	SLB、WAF、EIP（含NAT网关公网IP） 实例
华东1（杭州）	500 M	1 G	5 G	5 G
华东2（上海）	500 M	1 G	2 G	2 G

地区	1 核 CPU 规格 ECS 实例	2 核 CPU 规格 ECS 实例	4 核以上 CPU 规格 ECS 实例	SLB、WAF、EIP（含NAT网关公网IP） 实例
华北1（青岛）	500 M	1 G	5 G	5 G
华北2（北京）	500 M	1 G	2 G	2 G
华北3（张家口）	500 M	1 G	2 G	2 G
华北5（呼和浩特）	500 M	1 G	2 G	2 G
华南1（深圳）	500 M	1 G	2 G	2 G
西南1（成都）	500 M	1 G	2 G	2 G
中国香港	500 M	500 M	500 M	500 M
新加坡	500 M	500 M	500 M	500 M
澳大利亚（悉尼）	500 M	500 M	500 M	500 M
马来西亚（吉隆坡）	500 M	500 M	500 M	500 M
印度尼西亚（雅加达）	500 M	500 M	500 M	500 M
日本（东京）	500 M	500 M	500 M	500 M
德国（法兰克福）	500 M	500 M	500 M	500 M
英国（伦敦）	500 M	500 M	500 M	500 M
美国（硅谷）	500 M	1 G	2 G	2 G
美国（弗吉尼亚）	500 M	500 M	500 M	500 M
印度（孟买）	500 M	1 G	1 G	1 G
阿联酋（迪拜）	500 M	500 M	500 M	500 M

默认的黑洞时长是2.5个小时，黑洞期间不支持解封。 实际黑洞时长视攻击情况而定，从30分钟到24小时不等。黑洞时长主要受以下因素影响：

- 攻击是否持续。如果攻击一直持续，黑洞时间会延长，黑洞时间从延长时刻开始重新计算。
- 攻击是否频繁，如果某用户是首次被攻击，黑洞时间会自动缩短；反之，频繁被攻击的用户被持续攻击的概率较大，黑洞时间会自动延长。

 说明：

针对个别黑洞过于频繁的用户，阿里云保留延长黑洞时长和降低黑洞阈值的权利，具体黑洞阈值和黑洞时长以控制台显示为准。

查看各实例的实际黑洞阈值

您可以参考以下步骤在云盾管理控制台中查看您已购买的的ECS、SLB或EIP实例的实际黑洞阈值：

1. 登录云盾DDoS基础防护管理控制台。
2. 选择地域。
3. 在基础防护 > 实例页面，选择要操作的实例类型：ECS、SLB、EIP（含NAT）。
4. 在实例列表选择要查看的实例，查看其当前防护阈值。

3.9 云虚拟主机DDoS防护黑洞阈值

云独享虚拟主机默认黑洞触发阈值如下（单位：bps）。

说明:

对于共享虚拟主机，由于多台共享虚拟主机会共享同一个IP，因此其黑洞阈值无法确定，但必定低于同地域独享虚拟主机的黑洞阈值。而且，如果有一台共享虚拟主机遭受大量DDoS攻击并触发黑洞机制，那么与它共享IP的其他虚拟主机都将无法访问。如果您的业务对安全性和稳定性有一定要求，建议购买独享虚拟主机或者ECS云服务器。

地区	独享虚拟主机
华东 1（杭州）	5G
华北 1（青岛）	5G
华南 1（深圳）	2G
华北 2（北京）	2G
华东 2（上海）	2G
中国香港	500M
美国	500M
新加坡	500M

默认的黑洞时长是2.5小时，黑洞期间不支持解封。实际黑洞时长视攻击情况而定，从30分钟到24小时不等。黑洞时长主要受以下因素影响：

- 攻击是否持续。如果攻击一直持续，黑洞时间会延长，黑洞时间从延长时刻开始重新计算。
- 攻击是否频繁，如果某用户是首次被攻击，黑洞时间会自动缩短；反之，频繁被攻击的用户被持续攻击的概率较大，黑洞时间会自动延长。

说明：

针对个别黑洞过于频繁的用户，阿里云保留延长黑洞时长和降低黑洞阈值的权利，具体黑洞阈值和黑洞时长以控制台显示为准。

如果您想获得更高的增量DDoS防护能力，购买DDoS高防IP服务，获得每天最高300G的独享DDos防护服务。

3.10 云产品规格与清洗阈值

阿里云免费为您提供基础DDoS防护能力，帮助您缓解面向公网开放的云产品所遭受的DDoS攻击。当云产品公网IP的网络流量超过设置的清洗阈值时，DDoS基础防护服务将自动对该IP的流量进行清洗，尽可能地保障您的正常业务免受DDoS攻击影响。

关于流量清洗的详细说明，请参见流量清洗、黑洞与阈值。

其中，各云产品所支持设置的最大清洗阈值取决于各云产品实例的规格。在您创建或变更云服务器ECS、负载均衡SLB、NAT网关实例时，系统将自动计算当前实例规格所对应的最大清洗阈值。

说明：

各云产品实例的实际黑洞阈值将综合最大清洗阈值、安全信誉等因素进行计算。

- 关于云服务器ECS实例的最大清洗阈值的具体计算方式，请参见云服务器ECS DDoS基础防护。
- 关于负载均衡SLB实例的最大清洗阈值的具体计算方式，请参见负载均衡SLB DDoS基础防护。
- 关于NAT网关实例的最大清洗阈值的具体计算方式，请参见NAT网关 DDoS基础防护。

说明：

弹性公网IP（EIP）的最大清洗阈值的计算方式与NAT网关相同。

3.11 云服务器压力测试指引

云盾DDoS基础防护服务默认为云服务器提供DDoS攻击防御能力。默认情况下，当云服务器的网络流量超过每秒180M流量、每秒30,000个报文数、每秒480个HTTP请求中的任何一项（根据实际实例规格可能有所不同），云盾将自动启动DDoS防御服务对流量进行清洗。

因此，您在对云服务器进行压力测试前，需要在云盾DDoS基础防护管理控制台调整目标云服务器实例的DDoS防护阈值。具体操作方式，参考设置清洗阈值。

说明:

强烈建议您每分钟的压力测试增长速度不要超过100倍，否则仍可能触发流量清洗。

3.12 通过设置白名单解决因误判IP被拦截问题

若您发现部分正常业务或者 IP 无法访问，有可能是因为攻击误判导致 IP 被拦截,。

背景信息

例如，您的网络环境为 NAT 环境（即局域网内相关主机共享公网 IP 上网），由于局域网内部分主机因中病毒或被入侵后对外攻击某 ECS 服务器，被云盾识别后，会对相应的 NAT 共享公网 IP 进行拦截，从而导致无法访问。

您可以通过设置白名单放行因误判导致的 IP 被拦截问题。

操作步骤

1. 登录云盾安全管控平台管理控制台。

   说明:

   您也可以在登录阿里云控制台后，将鼠标移至右上角的账户图标打开用户菜单，并单击安全管控，进入云盾安全管控平台管理控制台。

2. 定位到白名单管理 > 访问白名单页面，单击添加。
3. 选择对象类型，输入源IP（非当前云账户名下的IP），在左侧列表中选择当前云账号名下的对象IP（例如ECS云服务器公网IP），单击右箭头按钮，将选中的IP加入右侧待添加列表，单击确定。即将所输入的访问源IP加入所添加的对象IP的访问白名单，所有来自该源IP对于您云账户名下的目标IP的访问都将不受任何安全管控限制。

   说明:

如果您想要放行所有对该对象IP的访问，在源IP框中输入0.0.0.0即可放行所有IP对该目标IP的访问。

来自访问白名单中的源IP对目标主机资产的访问将不受任何安全管控限制，即使访问可能是有风险的也不会进行任何安全管控限制。因此，请务必谨慎添加访问白名单。

说明:

IP添加至访问白名单后，将在10分钟内正式生效。

4 常见问题

4.1 云盾攻击扫描拦截全局白名单添加申请

阿里云为用户提供了安全的云环境，可以做到实时阻断黑客攻击行为。由于部分CDN或类似功能产品可能具有请求转发行为，转发时因带有源IP请求的攻击行为触发云盾防御均会导致访问异常。

考虑到部分阿里云用户对这类产品的需求，CDN厂商（简称“申请厂商”）可以通过以下方式为其相关产品申请添加拦截基础防护全局白名单，从而避免以上情况。

> 说明:
> 如果只需要针对您自己的ECS云服务器设置访问白名单，查看通过设置白名单解决因误判IP被拦截问题。

请申请厂商撰写一封公函，包含以下内容：

- 需要申请加白的IP地址列表（如果数量过多可以用相关地址的官方链接替代，同时请在邮件附件中以表格形式发送）
- IP地址用途说明
- 申请厂商承诺遵守适用的相关法律法规。同时，申请厂商承诺不对阿里云以及阿里云的用户发起任何形式的攻击。如果因申请厂商添加到白名单中的IP地址威胁到阿里云安全或阿里云用户安全或者涉嫌其它违法、违规行为，阿里云有权采取将IP地址移出白名单的操作，申请厂商应对由此产生的后果承担全部责任，如给阿里云造成损失的，并应赔偿阿里云的全部损失。
- 联系方式（电话或者旺旺等）
- 加盖公司公章

请以公司名义将申请厂商的营业执照电子扫描件连同上述公函的电子扫描件以邮件形式发送到以下邮箱地址：

- To: dachao.xdc@alibaba-inc.com
- Cc: yemin.ym@alibaba-inc.com

获取授权

阿里云将在两个工作日针对该申请进行初次非自动的回应。在阿里云审核申请厂商的申请材料过程中如有任何疑问阿里云有权要求申请厂商阐明。请注意，审核申请过程可能需要几个工作日，因此请做好相应安排。当资料审核完成后阿里云将回复申请厂商审核结果。

同时，请申请厂商知晓，阿里云会根据一定策略定期清理该白名单列表，如有相关产品IP地址调整或变更，请及时与阿里云联系并告知具体情况。如果阿里云发现申请厂商添加到白名单中的IP地址威胁到阿里云用户安全，阿里云会把该IP地址从白名单中永久删除并保留追究相关法律责任的权利。

4.2 DDoS防护常见问题

目前，每台云服务器都是默认启动DDoS基础防护服务。单台云服务器流量超过一定流量时将自动启动DDoS清洗设备进行流量清洗。

DDoS基础防护可以防syn攻击吗?

DDoS基础防护服务可以防御syn洪水攻击。

查看DDoS防护情况的周期可以选择吗?

云盾DDoS基础防护控制台支持24小时内的DDoS攻击事件查询，需要更长周期请查看态势感知。

我的ECS服务器被20Mb的流量攻击了，云盾DDoS基础防护怎么不防护?

云盾DDoS基础防护是公共的DDoS防护服务，不对很小的流量攻击（小于100Mb）进行防护。建议您优化服务器性能，或者安装云锁等主机防火墙应对小于100Mb的流量攻击。

为什么黑洞不能立即取消?

绝大多数用户的黑洞时间在30分钟到24小时之间。如果一个用户的攻击很频繁，阿里云可能通过增加黑洞事件采取惩罚措施。

黑洞是阿里云向运营商购买的服务，运营商有明确的黑洞解除时间限制，所以一般情况下黑洞不能立即取消。