阿里云
DDoS防护

DDoS原生防护

文档版本：20200707

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。
斜体	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 开通DDoS原生防护企业版

本文介绍了开通DDoS原生防护企业版实例的操作步骤。

前提条件

DDoS原生防护-企业版仅向已完成企业实名认证的用户开放。在开通服务前，您必须先在DDoS原生防护-企业版申请页面提交购买申请。

背景信息

DDoS原生防护（防护包）提供基础版和企业版套餐。

- 基础版：默认为阿里云资源公网IP免费开启，无需购买。提供不超过5 Gbps的DDoS基础防护能力。
- 企业版：购买后开启，支持防护阿里云资源公网IP，例如ECS、SLB、EIP、WAF。提供不改变IP地址的DDoS共享全力防护能力。全力防护指阿里云根据当前机房网络的整体水位，尽可能帮助您防御DDoS攻击。随着阿里云网络能力的不断提升，全力防护的防护能力也会相应提升，而不需要您额外付出升级成本。

  关于DDoS原生防护的详细计费说明，请参见#unique_4。

操作步骤

1. 访问阿里云DDoS高防IP产品详情页并登录您的阿里云账号。
2. 单击**立即购买**。
3. 在**DDoS高防（新BGP）**购买页面，单击**DDoS原生防护（防护包）**页签。

4. 在**DDoS原生防护（防护包）**购买页面，完成实例配置。DDoS原生防护实例的配置描述如下。

配置项	说明
防护套餐	选择**企业版**。
IP协议	原生防护实例支持防护的IP协议类型，可选值：**IPv4**、**IPv6**。
资源所在地域	原生防护实例的地域。 **注意：** DDoS原生防护实例的地域必须与要绑定的防护对象（例如ECS、SLB等云产品）所在的地域一致。
资源组	原生防护实例的资源组。

配置项	说明
业务规模	要防护业务的正常业务规模，以带宽来衡量。可选值：100 Mbps、300 Mbps、500 Mbps、800 Mbps、1 Gbps、1.5 Gbps、2 Gbps、2.5 Gbps、3 Gbps。 关于业务规模的估算方法，请参见#unique_4/unique_4_Connect_42_section_y6r_x7v_t68。
保护IP数量	要防护的IP的总数，取值范围：100~255。默认值为100。
购买数量	要开通的原生防护实例的总数。 **说明：** 建议您根据当前地域下需要保护的IP数量决定购买实例的数量。例如，如果设置每个实例防护200个IP地址，而需要保护的IP总数量为400个，则您可以购买两个实例。
订购时长	要开通的原生防护实例的有效期。

5. 单击**立即购买**。
6. 完成支付。

预期结果

成功开通DDoS原生防护-企业版实例后，您可以在DDoS原生防护实例页面查看已开通的实例。

后续步骤

为遭受攻击的IP开通DDoS原生防护

2 资产中心

DDoS原生防护基础版默认开启，免费为您阿里云账号下的ECS、SLB和EIP实例提供不超过5 Gbps流量的DDoS攻击防护能力。DDoS防护资产中心向您展示阿里云账号下已开通资产（包括ECS、SLB、EIP等）的DDoS防护状态和流量趋势，帮助您快速了解资产的DDoS安全风险，并支持为指定资产提升DDoS防护能力。

操作步骤

1. 登录云盾DDoS防护产品控制台。
2. 在**资产中心**页面上方选择资产所在地域。
3. 在**资产中心**页面查看**DDoS攻击防护说明**。

DDoS攻击防护说明中支持以下操作：

- 单击**默认基础防护阈值**，查看不同地域下资产的默认DDoS防护能力，即支持防御的DDoS攻击带宽。
- 单击**黑洞**，查看阿里云黑洞策略。
- 单击**DDoS原生防护**，前往DDoS原生防护**实例管理**页面，您可以根据需要开通DDoS原生防护实例。更多信息，请参见开通DDoS原生防护企业版。

4. 单击对应页签，选择要操作的云产品类型：**ECS**、**SLB**、**EIP（含NAT）**、**其他**。

> **说明：**
> **其他**指您所保有的DDoS原生防护代播实例。代播实例可以防护海外线下IDC服务器或云上资产通过网段实现DDoS原生防护，支持通过控制台或API的方式手动开启和关闭防护。更多信息，请参见#unique_7。

5. 在资产列表查看资产的DDoS防护状态。

   资产中心页面展示了当前地域下所有资产的DDoS防护信息，具体包括**状态**、**防护能力**、**清洗阈值**。

   - **状态**表示实例的DDoS安全状态，分为**正常**、**清洗中**、**黑洞中**。
     - 如果实例状态为清洗中，您可以手动取消流量清洗。更多信息，请参见取消流量清洗。
     - 如果实例状态为黑洞中，您可以查看黑洞事件记录。更多信息，请参见查看IP进入黑洞的时间和原因。
   - **防护能力**表示实例的DDoS攻击防护能力，即可以防御的最大攻击带宽。如果攻击带宽超过了当前实例的防护能力，则实例将会进入黑洞。您可以参照步骤5为指定实例提升DDoS防护能力。
   - **清洗阈值**表示触发流量清洗的最小访问带宽，体现在流量（Mbps）和报文数量（PPS）。更多信息，请参见设置清洗阈值。

6. 为指定资产提升DDoS防护能力。

   - 添加DDoS原生防护

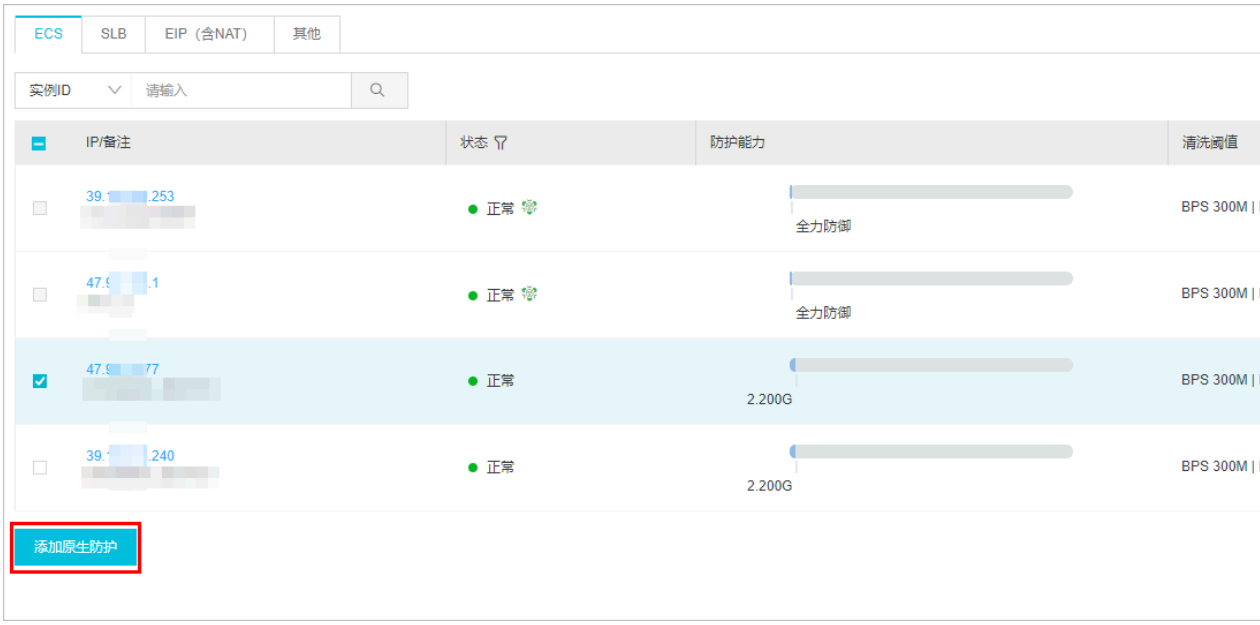
     如果您在当前地域下已开通付费版原生防护实例，则您可以参照以下步骤为指定资产开启原生防护。

     DDoS原生防护（企业版）为您提供账号级、全资产、全业务的DDoS防护，缓解企业在云上面临的DDoS攻击风险，降低DDoS可能导致的业务中断风险。针对企业提供费用可控、无需改变

业务架构、无延迟增加、支持大型业务的防护。更多信息，请参见什么是DDoS原生防护（防护包）。

为不同类型资产（ECS、SLB、EIP）开启原生防护的操作基本类似，以下以ECS为例介绍为资产开启原生防护的操作步骤，其它类型资产可作参考。

a. 在ECS实例列表中勾选要操作的实例，并单击列表下方的**添加原生防护**。



b. 在**DDoS原生防护列表**，选择要应用的原生防护实例，单击其操作列下的**添加**。

c. 在**确认**对话框中，单击**确定**。

- 开通DDoS高防服务

  如果您的业务面临高风险的DDoS攻击，例如发生频率高、攻击流量大、业务影响严重等，建议您为资产开通DDoS高防服务。

  DDoS高防服务采用中国大陆地域独有的T级八线BGP带宽资源，可以帮助您防御超大流量DDoS攻击。更多信息，请参见#unique_12。

  您可以在左侧导航栏**DDoS高防**目录下单击**DDoS高防（新BGP）**或者**DDoS高防（国际）**，直达对应的产品控制台。

  - DDoS高防（新BGP）适用于部署在中国内地地域的业务。
  - DDoS高防（国际）适用于部署在中国内地以外地域的业务。

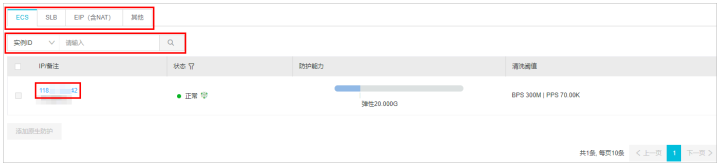
3 设置清洗阈值

云盾DDoS防护为您的阿里云资产（包括ECS、SLB、EIP等）免费提供DDoS基础防护能力，资产开通后默认启用DDoS防护。当IP遭受的DDoS攻击带宽超过清洗阈值时，DDoS防护对攻击流量进行清洗，并尽可能保障您的业务可用。本文介绍了为指定资产设置DDoS防护清洗阈值的操作方法。

操作步骤

1. 登录云盾DDoS防护产品控制台。
2. 在**资产中心**页面上方选择资产所在地域。
3. 单击对应页签，选择要操作的云产品类型：**ECS**、**SLB**、**EIP（含NAT）**、**其他**。
4. 在实例列表中定位到要操作的实例，单击其**IP**。

   如果实例过多，建议您使用**实例ID**、**实例名称**或**实例IP**搜索目标实例。



5. 在**实例详情**侧边页，单击**清洗设置**。

6. 在**清洗设置**侧边页，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。

   清洗阈值设置建议：

   - 清洗阈值需要略高于实际访问值。阈值设置过高，起不到防御效果；而设置过低，DDoS防护触发流量清洗可能会影响正常的访问。
   - 如果清洗影响了正常的请求，请适当调高清洗阈值。
   - 在网站做推广或者活动时，建议您适当调大清洗阈值。

预期结果

成功设置清洗阈值。当网站请求达到设置的清洗阈值时，DDoS防护将触发流量清洗。

4 取消流量清洗

云盾DDoS防护默认为阿里云服务器提供DDoS攻击防御能力。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。对于处于异常状态（清洗中）的IP资产，您可以手动取消流量清洗。

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。

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防护产品控制台。
2. 在**资产中心**页面上方选择资产所在地域。
3. 单击对应页签，选择要操作的云产品类型：**ECS**、**SLB**、**EIP（含NAT）**、**其他**。
4. 在实例列表中定位到要操作的实例（**状态**为**清洗中**），单击其**IP**。
5. 在**实例详情**侧边页，定位到进行中的清洗事件（**事件**为**清洗**且**结束时间**为空），单击其操作列下的**取消清洗**。

说明：

如果当前没有进行中的清洗事件，则**取消清洗**操作不会出现。

预期结果

成功取消流量清洗。

后续步骤

取消流量清洗后，建议您根据当前业务需要（例如活动或大促期间业务访问量增大）适当调高清洗阈值，避免再次触发流量清洗。更多信息，请参见设置清洗阈值。

说明:

最大清洗阈值和云产品实例的规格绑定。如果可配置的最大清洗阈值无法满足您的需求，建议您升级云产品规格。

5 黑洞策略

5.1 查看黑洞时长

服务器遭受DDoS攻击触发黑洞后，其公网IP在一定时间内将无法被访问，只有等到黑洞时长过后才会恢复正常访问。不同地域资产的默认黑洞时长不同，且黑洞时长受资产遭受的攻击情况影响。您可以在DDoS防护控制台查看当前资产的黑洞时长。

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防护控制台显示为准，详见下文操作步骤。

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。

关于阿里云黑洞策略的更多信息，请参见#unique_15。

操作步骤

1. 登录云盾DDoS防护产品控制台。
2. 在**资产中心**页面上方选择资产所在地域。
3. 在资产列表上方查看**DDoS攻击防护说明**。

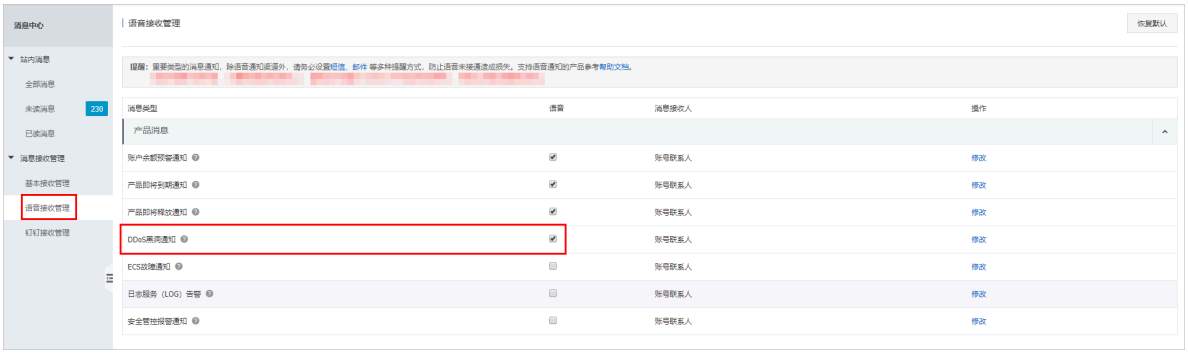
   DDoS攻击防护说明中的**当前黑洞解除时间**即当前地域下资产的黑洞时长

5.2 设置黑洞告警通知

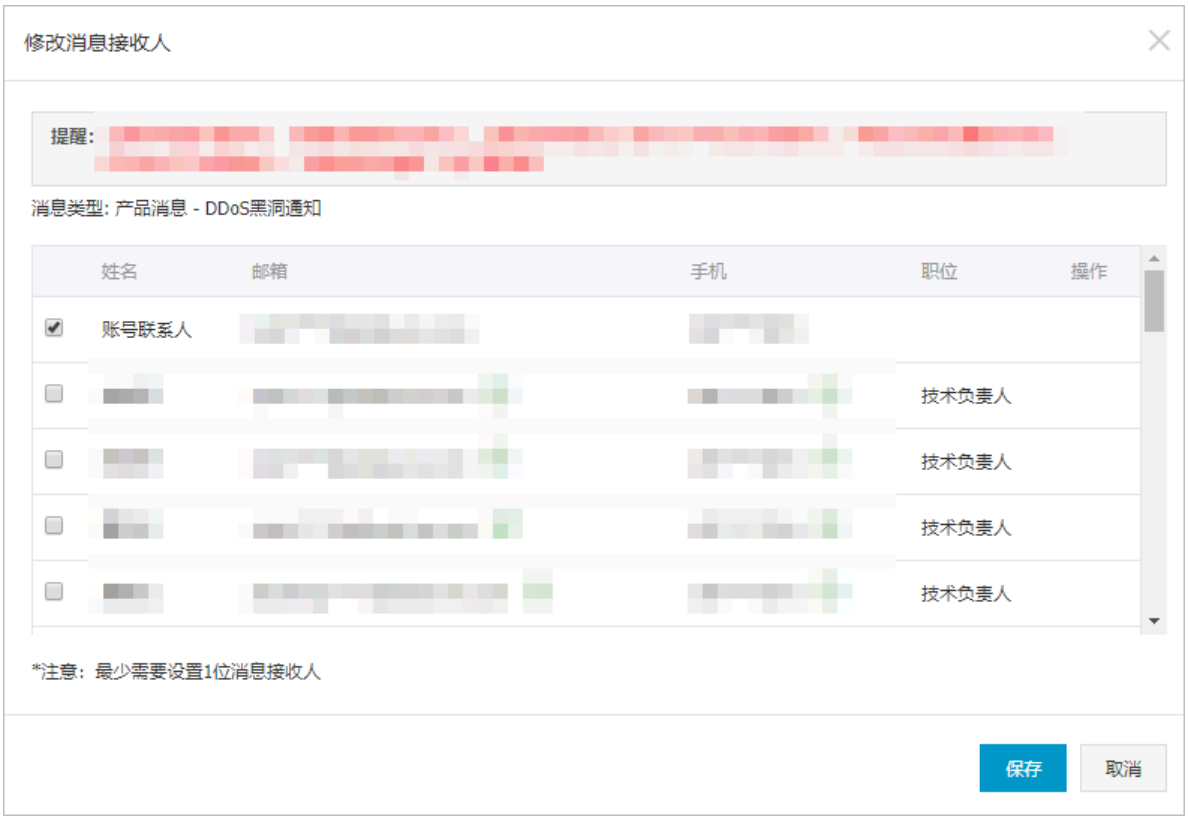
阿里云的DDoS黑洞通知提供告警通知功能。当您账号中的服务器遭受大量DDoS攻击触发黑洞时，您所设定的消息接收人将收到通知。

启用DDoS黑洞语音告警

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 > 语音接收管理**。
3. 定位到**DDoS黑洞通知**，勾选**语音**，启用语音告警功能。



4. 单击**DDoS黑洞通知**操作列下的**修改**，并在**修改消息接收人**对话框中添加、修改DDoS黑洞通知的消息接收人。



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。

5.3 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。您可以在云盾DDoS防护控制台查看账号下资产的黑洞事件信息，例如IP进入黑洞的时间及所遭受的攻击流量。

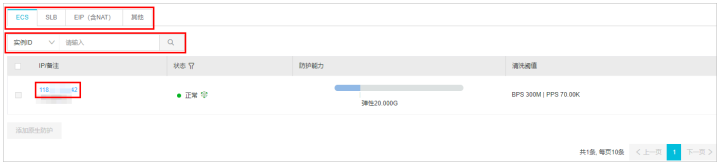
背景信息

不同地域下实例的黑洞阈值可能不同。关于黑洞的具体说明，请参见#unique_15。

操作步骤

1. 登录云盾DDoS防护产品控制台。
2. 在**资产中心**页面上方选择资产所在地域。
3. 单击对应页签，选择要操作的云产品类型：**ECS**、**SLB**、**EIP（含NAT）**、**其他**。
4. 在实例列表中定位到要操作的实例，单击其**IP**。

   如果实例过多，建议您使用**实例ID**、**实例名称**或**实例IP**搜索目标实例。



5. 在**实例详情**侧边页，通过事件列表查看历史黑洞事件（**事件**为**黑洞**）的信息，并在流量图中查看黑洞事件发生时的攻击流量。

   黑洞事件中记录了黑洞的**开始时间**和**结束时间**。

说明：

如果当前资产中未发生过黑洞/清洗事件，则事件列表中将无记录展示。

6. （可选） 单击目标事件操作列下的**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，用于向网监报案。

5.4 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_18。

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。

5.5 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、EIP、WAF实例，且适用于IPv4和IPv6环境的防护，但部分地区暂不支持IPv6防护。在下表中的支持IPv6列，√表示该地区支持IPv6防护，防护阈值同时适用于IPv4和IPv6；×表示该地区暂不支持IPv6防护，防护阈值仅适用于IPv4。
- ECS、SLB、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，具体以云盾DDoS防护产品控制台的**资产中心**页面显示为准。更多信息，请参见资产中心。
- WAF实例IP的黑洞阈值与SLB、EIP实例一致。

地区	支持IPv4	支持IPv6	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、EIP（含NAT网关公网IP）、WAF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
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
华南2（河源）	√	√	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

地区	支持IPv4	支持IPv6	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、EIP（含NAT网关公网IP）、WAF实例
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。

5.6 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。

5.7 解除黑洞

DDoS原生防护（防护包）为已防护的IP提供黑洞解除功能，您可以对某个处于黑洞状态的防护对象IP进行黑洞解除操作。

背景信息

购买DDoS原生防护（防护包）企业版的用户将获赠100次黑洞解除机会。在您已开通的DDoS原生防护实例的服务周期内，每月初该防护包实例的黑洞解除次数将自动重置为100。

说明：

上月未使用的剩余黑洞解除次数将不会累计至下月。

强烈建议您在执行黑洞解除操作前查看平台自动解封时间，如果您可以接受该自动解封时间，请您耐心等待平台自动解封。更多信息，请参见查看黑洞时长。

操作步骤

1. 登录云盾DDoS防护产品管理控制台。
2. 在页面上方选择原生防护实例的地域。
3. 在**DDoS原生防护**页面，定位到要操作的原生防护实例，单击其操作列下的**解除黑洞**。

> **说明：**
> 只有当原生防护实例下存在**异常IP**（即防护对象被黑洞）时，才支持**解除黑洞**操作。

4. 在**防护对象**页签下，定位到处于**黑洞中**状态的防护对象，单击其操作列下的**解除黑洞**。

5. 在**解除黑洞**对话框，查看剩余黑洞解除次数，并单击**确认**。

> **说明：**
> 由于黑洞解除涉及阿里云后台系统的风控管理策略，解除黑洞操作可能失败（解除失败时不会扣减您的剩余黑洞解除次数）。

预期结果

如果黑洞解除失败，您将收到失败提示信息，请耐心等待一段时间后再尝试。如果未收到提示信息，则表示黑洞状态已成功解除。

6 添加防护对象

开通DDoS原生防护（防护包）企业版后，您可以将需要防护的IP添加至DDoS原生防护实例进行防护。

操作步骤

1. 登录云盾DDoS防护产品管理控制台。
2. 在页面上方选择原生防护实例的地域。
3. 在**DDoS原生防护**页面，定位到要应用的原生防护实例，单击其操作列下的**添加防护对象**。

4. （可选）根据页面提示完成云产品授权，授权DDoS原生防护实例访问您的其他云产品对象。

> **说明：**
> 只有当您第一次使用DDoS原生防护实例时，才会出现授权提示页面。如果您已经完成授权，则不会出现提示页面。

5. 在**添加防护对象**对话框，输入您想要防护的云产品的IP，并单击**确定**。

完成防护配置后，DDoS原生防护实例将直接为您所添加的防护对象IP提供DDoS防护能力。

添加防护IP时，如果您收到**IP不属于你**的错误提示，请参见添加防护对象IP报错问题。

相关操作

- 查看安全报表
- 解除黑洞

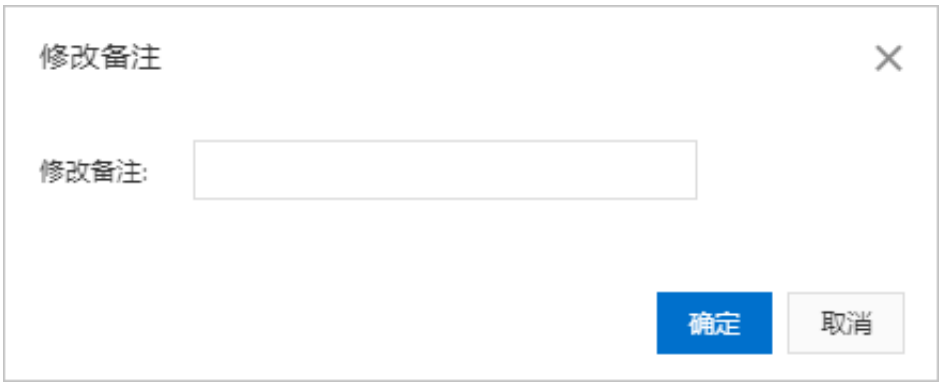
7 设置实例的备注名称

DDoS原生防护（防护包）实例支持设置备注名称。当拥有多个DDoS原生防护实例时，您可以根据原生防护实例的使用对象、场景、范围等设置备注名称，用于区分不同用途的原生防护实例，并可通过备注名称快速辨识和管理您的原生防护实例。

操作步骤

1. 登录云盾DDoS防护产品管理控制台。
2. 在页面上方选择原生防护实例的地域。
3. 在**DDoS原生防护**页面，定位到要操作的实例，单击其备注名后的编辑图标。

4. 在**修改备注**对话框，输入原生防护实例的备注名称，并单击**确认**。



预期结果

设置成功后，备注名称将显示在DDoS原生防护实例ID下方。您也可以按照上述步骤随时修改DDoS原生防护实例的备注名称，根据业务需要灵活地调整备注名称。

8 查看安全报表

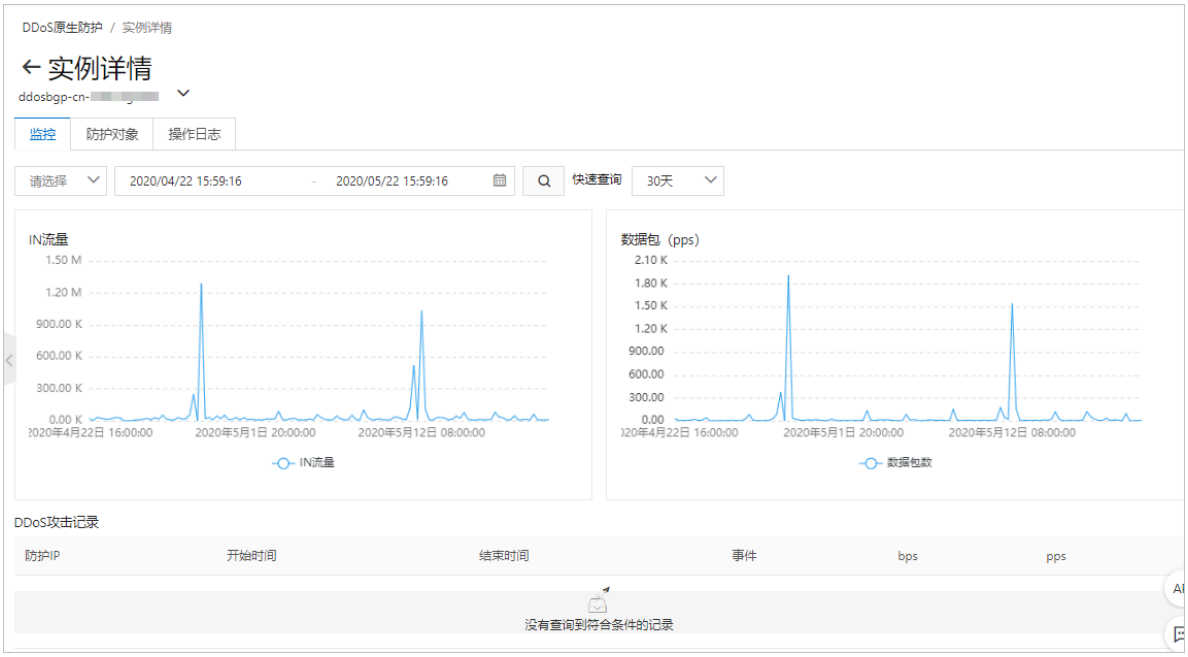
为DDoS原生防护实例配置完防护IP后，您可以查看原生防护实例的总流量信息、单个IP的流量信息和DDoS攻击事件记录。

操作步骤

1. 登录云盾DDoS防护产品管理控制台。
2. 在页面上方选择原生防护实例的地域。
3. 在**DDoS原生防护**页面，定位到要操作的原生防护实例，单击其操作列下的**查看报表**。

4. 在**监控**页签下，选择要查询的防护对象和时间范围，查看防护对象上的网络流量趋势（入方向流量和接收的数据包数）及DDoS攻击事件记录。

> **说明:**
> 支持查询近30天的数据。



9 查看操作日志

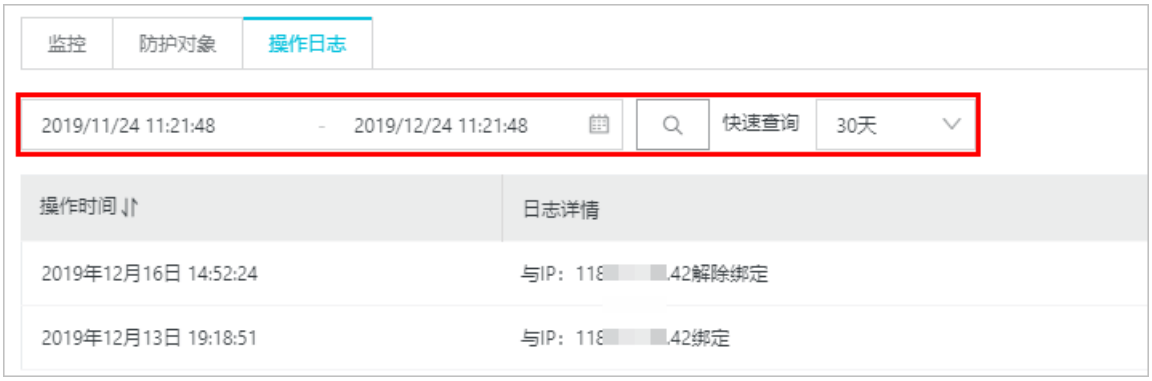
在云盾DDoS防护管理控制台，您可以查看DDoS原生防护（防护包）实例的操作日志，便于您追溯原生防护实例的配置变更情况。

操作步骤

1. 登录云盾DDoS防护产品管理控制台。
2. 在页面上方选择原生防护实例的地域。
3. 在**DDoS原生防护**页面，定位到要操作的原生防护实例，单击其操作列下的**管理**。

4. 在实例详情页面，单击**操作日志**页签。
5. 在**操作日志**页签下，设置要查询的时间范围，查看指定时间范围内该DDoS原生防护实例的操作日志，包括操作时间、操作日志详情。

> **说明:**
> 支持查看最近30天内的操作日志。



10 DDoS原生防护（防护包）升级DDoS高防IP

鉴于DDoS原生防护（防护包）服务的架构限制，在某些特定情况下，DDoS原生防护提供的安全防护能力可能无法完全满足您的DDoS防护需求。如果DDoS原生防护已无法满足您的安全防护需求，建议您切换至DDoS高防IP服务提升安全防护能力。

背景信息

关于DDoS原生防护适用的安全防护场景，请参见DDoS原生防护应用场景。

如果您已购买DDoS原生防护实例，在实际使用过程中遇到以下问题，可以将已购买的DDoS原生防护服务升级为DDoS高防IP服务：

- 遭受的DDoS攻击持续时间较长，且攻击流量较大。
- 防护的业务遭受CC攻击，而对此类攻击DDoS原生防护服务无法防御。
- 其他特殊情况，需要您具体说明。

> **说明：**
> DDoS原生防护（防护包）升级为DDoS高防IP服务时，对于您已购买的DDoS原生防护实例，我们将为您退回余款。

如果单独使用DDoS原生防护（防护包）/DDoS高防IP无法满足您的DDoS防护需求，推荐您组合使用DDoS原生防护和DDoS高防IP服务。更多信息，请参见DDoS原生防护和高防组合使用方案。

操作步骤

1. 通过您的专属服务钉钉群联系服务人员，说明详细情况。

   如果您尚未加入专属服务钉钉群，使用钉钉扫描下方二维码。

   > **说明：**
   > 如果在DDoS原生防护服务升级DDoS高防IP服务过程中遇到任何问题，请通过您的专属钉钉服务群联系服务人员。

2. 服务人员将根据您的实际情况判断是否满足升级条件。
3. 待服务人员确认满足升级条件后，将为您处理已购买的DDoS原生防护实例的退款事宜。系统将根据您所购买的DDoS原生防护实例的规格及剩余服务时长为您退回余款。
4. 购买DDoS高防IP实例，将您的业务切换至所DDoS高防IP实例进行防护。

11 为遭受攻击的IP开通DDoS原生防护

阿里云默认为您购买的所有具备公网IP的产品（ECS云服务器、SLB负载均衡、EIP弹性公网IP、Web应用防火墙）提供DDoS基础防护服务。当这些产品的公网IP遭受超过默认防护能力的DDoS攻击时，您可以立即付费开通DDoS原生防护（防护包），利用该公网IP所在地域的最大DDoS攻击防护能力防护攻击，保障您的业务免受攻击影响。

背景信息

DDoS原生防护企业版提供全力防护的弹性防护能力。当遭受攻击时，自动调度该企业版DDoS原生防护实例所在地域的阿里云最大DDoS防护能力提供全力防护。

准备工作

在购买开通DDoS原生防护（企业版）实例前，您应确认以下信息：

- 遭受攻击的IP地址。
- 遭受攻击的IP所在地域。

> **说明:**
> 目前，DDoS原生防护尚未在所有地域开通，因此您需要确认遭受攻击的IP所在的地域已开通DDoS原生防护服务。关于DDoS原生防护企业版支持的地域信息，请参见#unique_11。

操作步骤

1. 参见开通DDoS原生防护企业版，购买DDoS原生防护企业版实例。

   > **说明:**
   > 您所选择的DDoS原生防护的地域应与您需要防护的ECS、SLB、EIP等产品实例所在的地域一致。

2. 登录云盾DDoS防护产品管理控制台。
3. 在**DDoS原生防护**页面，参见添加防护对象，将需要防护的IP添加至已购买的DDoS原生防护实例中进行防护。

预期结果

防护IP添加成功后，该IP即可享受所绑定的DDoS原生防护实例的防护能力。您可以在**资产中心**页面查看到该IP的防护能力已经提升为所绑定的DDoS原生防护实例的防护能力。

12 最佳实践

12.1 DDoS原生防护（防护包）黑洞自动解除最佳实践

添加至DDoS防护包进行防护的业务IP遭受瞬时超大流量DDoS攻击时仍可能被黑洞，需要对被黑洞的IP快速执行黑洞解除操作恢复业务，保障业务稳定性。针对这一场景，企业版DDoS防护包提供黑洞自动化响应和快速解除的解决方案。

前提条件

DDoS防护包黑洞自动化响应和快速解除解决方案需要调用DDoS防护包的API接口，因此该解决方案仅支持企业版DDoS防护包实例。在部署黑洞自动解除方案前，请确认您的业务IP已添加至企业版DDoS防护包实例进行防护。更多信息，请参见添加防护对象。

背景信息

DDoS防护包提供黑洞解除功能，而手动解除黑洞（参见解除黑洞）可能存在延迟和不确定性。如果您的业务对于稳定性和连续性有较高的要求，您可以通过以下方案实现黑洞自动化响应和快速解除。

1. 通过云监控的事件告警功能监控DDoS防护包实例的黑洞事件。

   说明:
   只有已添加为DDoS防护包实例的防护对象IP触发黑洞策略时，才会触发云监控的黑洞事件报警的消息推送。对于不在DDoS防护包实例的防护对象列表中的IP触发的黑洞事件将不会被推送。

2. 通过自定义消息的消费机制，调用DDoS防护包的黑洞解除API接口（#unique_32）自动解除被黑洞的业务IP。

通过类似的方法，您还可以实现当DDoS攻击事件发生时自动调用云解析的API接口将相关域名的DNS解析切换至DDoS高防实例等。

操作步骤

1. 登录云监控控制台。
2. 在左侧导航栏，单击**报警服务** > **报警规则**。
3. 在**报警规则列表**页面，选择**事件报警**页签。

4. 单击**创建事件报警**，为DDoS防护包创建黑洞事件报警规则。

   - **产品类型**：选择**DDoS防护包**。
   - **事件名称**：选择**黑洞**。

5. 在所创建的事件报警中，根据您想要使用的消息消费机制，选择事件报警消息的推送渠道，并单击**确定**。

   云监控支持多种渠道供您实现事件消息的消费：

   - **消息服务队列**
   - **函数计算**
   - **URL回调**
   - **日志服务**

   事件报警创建完成后，当DDoS防护包实例中已防护的IP被黑洞时，云监控将自动报警并将以下消息实时推送至您所选择的消费渠道。

   消息示例

```
{
  "action": "add", //动作。其中，add表示事件开始；del表示事件结束。
  "bps": 0, //触发事件的流量bps，单位：Mbps。
  "pps": 0, //触发事件的包速率，单位：pps。
  "instanceId": "ddosbgp-cn-78v17******", //DDoS防护包实例ID。
  "ip": "47.*.*.*", //发生事件的IP。
  "regionId": "cn-hangzhou", //DDoS防护包实例所在的地域。
  "time": 1564104493000, //触发事件的时间，时间格式为毫秒时间戳。
  "type": "blackhole"  //事件类型。其中，defense表示清洗事件；blackhole表示黑洞事件。
}
```

6. 定义消息消费机制，对事件消息进行处理并结合#unique_32 接口实现黑洞自动解除。

12.2 DDoS原生防护和高防组合使用方案

通过组合使用DDoS原生防护（防护包）和DDoS高防，您可以在尽量保证正常业务流畅体验的前提下，为其部署强力的DDoS防护。组合使用方案通过DDoS高防流量调度器的防护调度规则实现。本文介绍了组合使用方案的配置方法。

背景信息

DDoS原生防护（防护包）是一款针对阿里云ECS、SLB、EIP、Web应用防火墙等云产品直接提升DDoS攻击防御能力的安全产品。DDoS原生防护的主要好处是可以直接把防御能力加载到云产品上，不需要更换IP，也没有四层端口、七层域名数等限制。DDoS原生防护部署简单，即刻购买，即刻生效，同时具备弹性防护能力，遭受大规模攻击时调用当前地域阿里云最大DDoS防护能力提供全力防护，可防御最高数百Gbps级别的DDoS攻击。

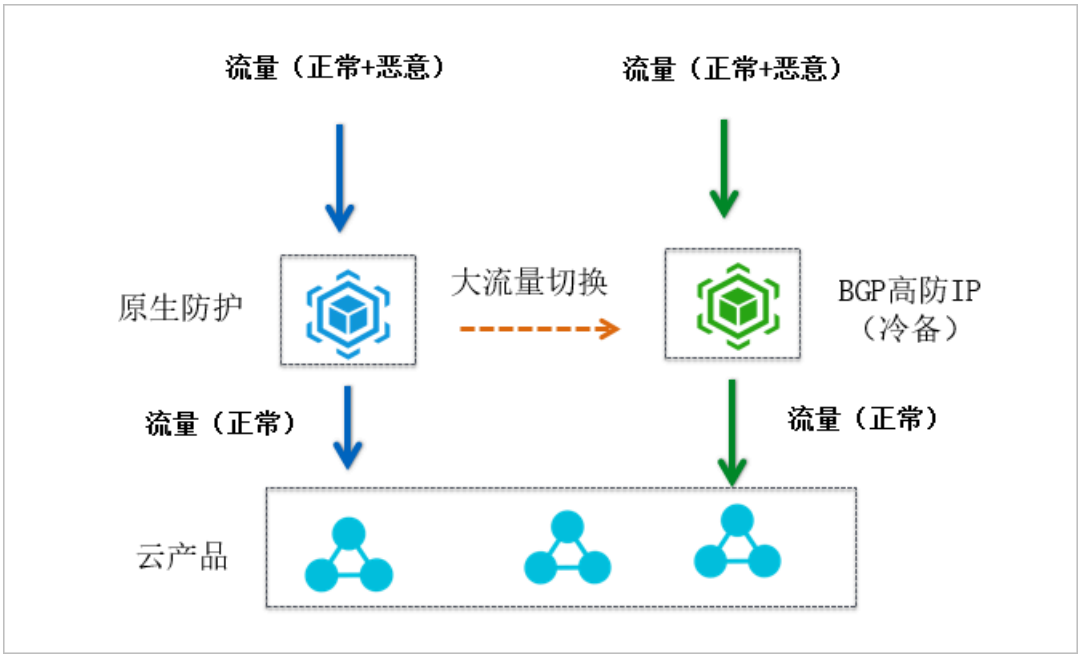
DDoS高防（新BGP）服务采用中国内地地域独有的T级八线BGP带宽资源，防护带宽最大达到1.5 T，可防御Tbps级别的超大流量DDoS攻击。DDoS高防采用DNS解析牵引的模式接入，拥有中国内地地域最优质的BGP带宽资源，BGP线路覆盖电信、联通、移动、教育等运营商线路，平均访问时延仅20 ms左右。

DDoS高防流量调度器允许您设置DDoS高防与DDoS原生防护之间的联动规则，实现日常使用原生防护防御DDoS攻击，仅在被大流量攻击的时候，切换到DDoS高防进行防御。

方案概述

DDoS原生防护和DDoS高防的组合方案允许您同时享受到DDoS原生防护和DDoS高防的优势，例如DDoS原生防护的费用可控、全资产防护、透明部署无延迟，和DDoS高防的超大攻击流量防护。

在DDoS原生防护和DDoS高防的组合方案中，您可以开通DDoS原生防护企业版，保护单地域255个IP，应用全力防护模式（防御能力一般不低于100~300 Gbps，具体和所在地域有关）；在DDoS原生防护的基础上，增加一组DDoS高防，冷备防御300 Gbps以上的大流量攻击。配置防护调度规则后，将业务接入高防流量调度器，在原生防护触发黑洞时自动切换DDoS高防IP。



DDoS原生防护和DDoS高防的组合方案具备以下特性：

- 原生防护企业版提供多区域、账号级DDoS防护，无需更改IP，无需改变业务架构，无延迟增加。
- 原生防护提供全力防护（防御能力一般不低于100~300 Gbps，具体和所在地域有关），300 Gbps以上的大流量自动切换到Tbps级别的高防防御。
- 黑洞触发自动切换，通过DNS调度完成切换，最短1~3分钟切换完成，最长5~10分钟全国切换完成。
- 专线回源，不受云产品黑洞影响。

部署组合方案后，业务默认解析在SLB、ECS、WAF，开启原生防护企业版，此时不增加延迟；攻击过大，原生防护触发黑洞时，高防调度器调度到DDoS高防IP，使用高防IP防御大流量的攻击，存在约20 ms的业务延时；攻击停止，流量回切到SLB、ECS、WAF，使用原生防护。

- 触发切换后，受国内local DNS影响，最多5~10分钟可以完成全国切换。

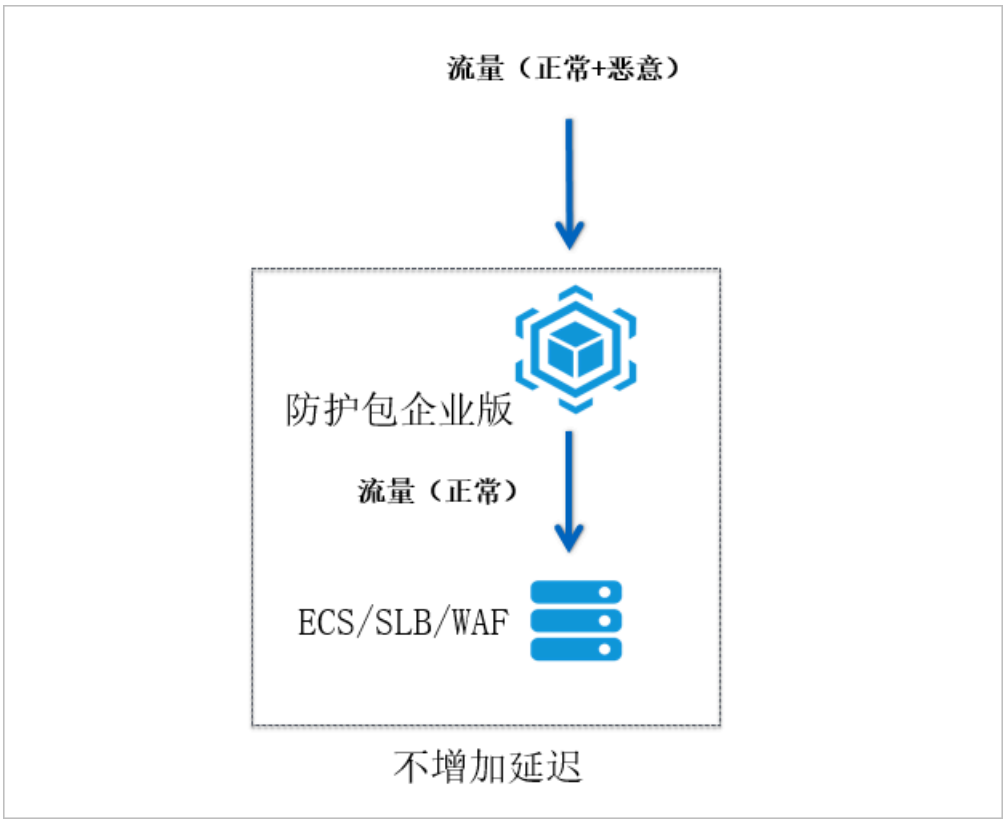
  说明：
  中国内地的DNS解析更新约需5~10分钟，非中国内地约需1~3分钟。
- 切换到DDoS高防时，黑洞阈值受高防的最大防护能力限制。开通实例时可以配置30 Gbps保底+300 Gbps弹性，但您可以通过工单联系我们升级到1 T甚至更高。
- 切换到高防之后，即使攻击停止也不会马上回切。流量调度器支持设置切换延迟时间，默认是120分钟（2小时），目的是防止回切后被持续攻击触发频繁切换，出现震荡，导致业务始终在切换状态。

开通和配置DDoS原生防护

开通DDoS原生防护（防护包）企业版实例，并添加同地域阿里云资源（ECS、SLB、EIP、WAF）作为防护对象。

注意：

- 如果采用公网SLB、ECS、EIP、NAT对外服务，需要注意对应产品的网络规格满足业务正常流量需要，并在DDoS基础防护控制台查看清洗限流阈值能否满足业务需求。
- 大促前，需要提前报备，协商正常流量峰值，防止误触发清洗或限流保护，对业务产生影响。



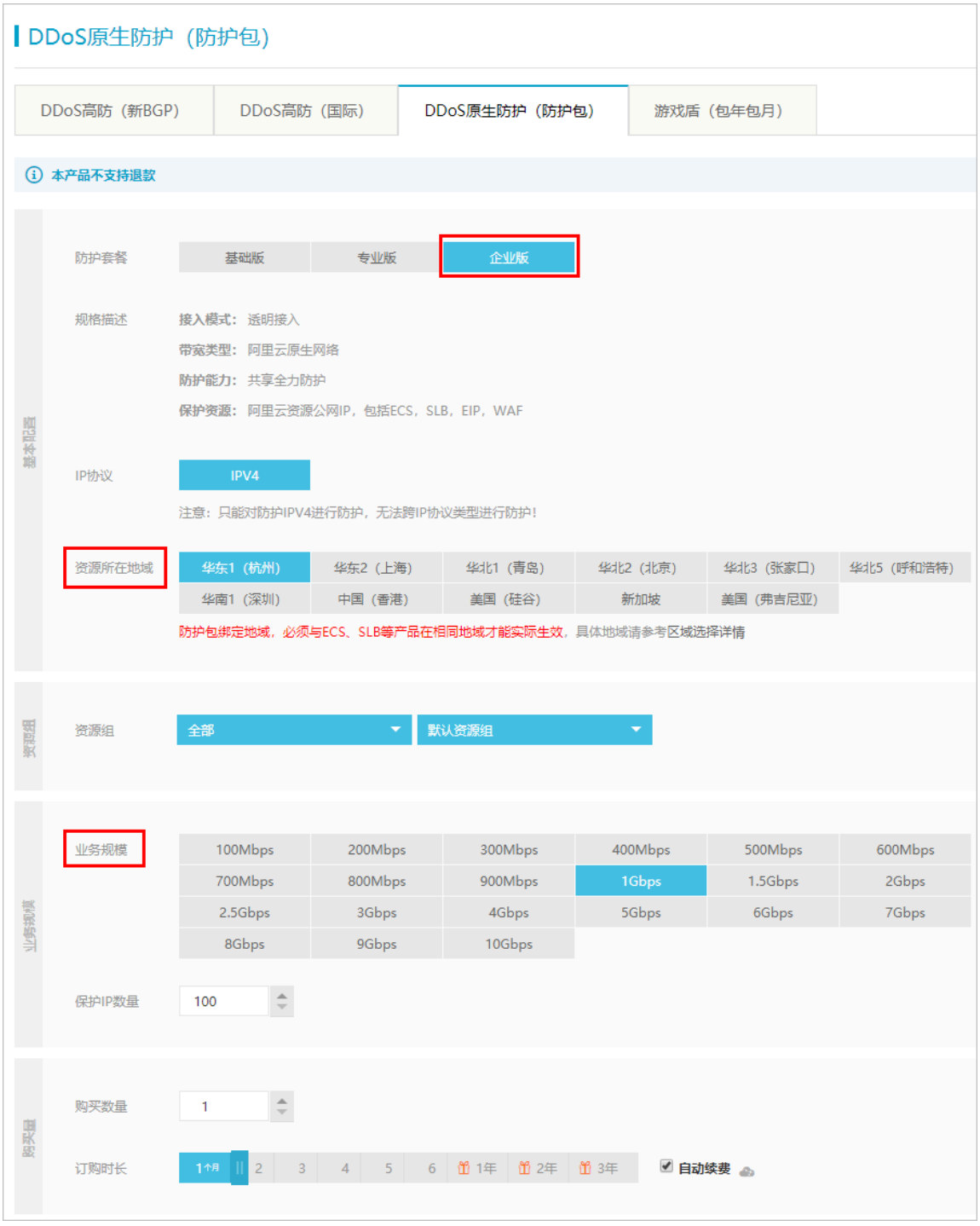
1. 开通DDoS原生防护企业版。若已开通，请跳过此步骤。

   a) 登录云盾DDoS防护产品管理控制台。

   b) 在**DDoS原生防护**页面，单击**新购原生防护**。

   c) 在**DDoS原生防护（防护包）**购买页面，完成防护包实例配置，并单击**立即购买**。防护包的配置描述如下。

   - **防护套餐**：**企业版**
   - **资源所在地域**：要防护的阿里云资源的地域
   - **业务规模**：要防护的业务的正常网络带宽



说明：

更多信息，请参见开通DDoS原生防护企业版。

d) 确认订单并完成支付。

2. 为DDoS原生防护添加防护对象。

   a) 登录云盾DDoS防护产品管理控制台。

   b) 在**DDoS原生防护**页面，定位到企业版防护包，单击其操作列下的**添加防护对象**。

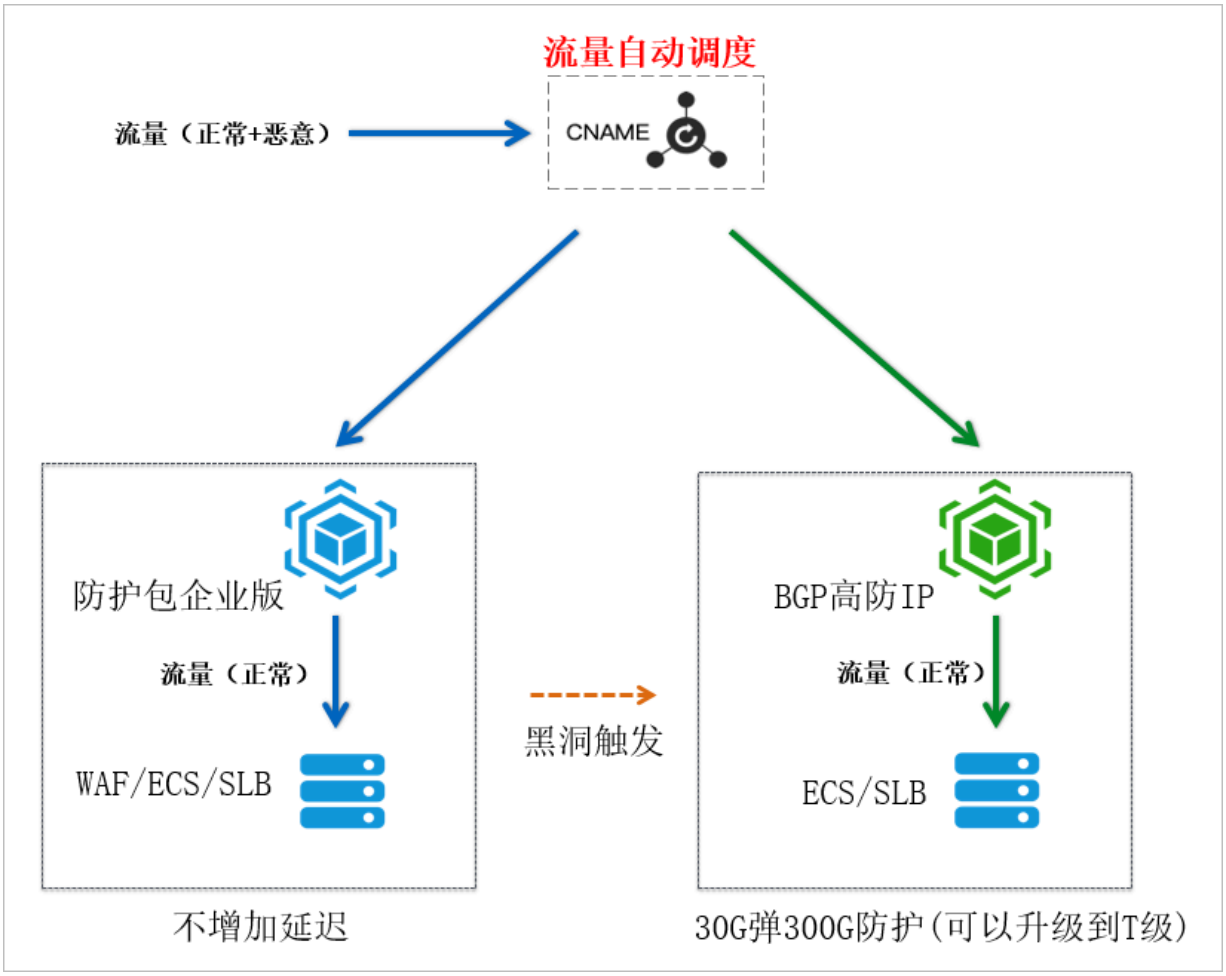
   c) 在**添加防护对象**对话框，输入要防护的业务的源站IP地址，并单击**确定**。

说明：

更多信息，请参见添加防护对象。

配置DDoS高防和流量调度器

开通DDoS高防（新BGP）专业版，添加业务转发规则，并通过流量调度器配置防护调度规则。完成规则配置后，将业务解析到流量调度器的Cname地址。


流量自动调度
流量（正常+恶意）
CNAME
防护包企业版
流量（正常）
WAF/ECS/SLB
黑洞触发
BGP高防IP
流量（正常）
ECS/SLB
不增加延迟
30G弹300G防护(可以升级到T级)

1. 开通DDoS高防专业版。若已开通，请跳过此步骤。

   a) 登录DDoS高防（新BGP）控制台。

   b) 在左侧导航栏，单击**资产管理** > **实例管理**。

   c) 单击**新购实例**。

   d) 在**DDoS高防（新BGP）**购买页面，完成高防实例的配置，并单击**立即购买**。高防实例的配置描述如下。

   - **防护套餐**：**专业版**
   - **保底防护带宽**：30 Gb
   - **弹性防护带宽**：300 Gb
   - **业务带宽**：要防护的业务的正常网络带宽


DDoS高防（新BGP）
新BGP高防IP
DDoS高防（国际）
游戏盾（包年包月）
本产品不支持退款。业务服务器在中国大陆，推荐购买新BGP高防，使用新BGP高防，域名必须经过ICP备案，未备案域名将无法正常访问。业务服务器在海外，推
基本配置
防护套餐
专业版
基础规格
接入模式： DNS解析牵引
资源预留： 1个独享 IP
带宽类型： 多线BGP
防护能力： 保底防护（预付费）+ 弹性防护（按量后付费）
保底防护带宽
30Gb
60Gb
100Gb
300Gb
400Gb
500Gb
600Gb
此部分为保底带宽，预付费。计费详情
弹性防护带宽
30Gb
40Gb
50Gb
60Gb
70Gb
80Gb
100Gb
150Gb
200Gb
300Gb
弹性防护带宽为最高防护带宽，如果弹性防护带宽值跟保底防护带宽值设置一样，则不会产生后付费且最高防护带宽为保底防护带宽值，如果弹性带宽值设置高于保底带宽值，则超过保底带宽值但不大于弹性带宽值的攻击仍然可以进行有效防护，但会根据超出保底带宽的部分产生后付费。请参考产品价格详情
业务带宽
2500M
5000M
1000 M
当您购买的套餐规格里的业务带宽不够用时，可能会丢包或者影响业务，在这种情况下请及时升级业务带宽。
资源组
资源组
全部
默认资源组
高级配置
功能套餐
标准功能
增强功能
防护域名数
50
防护域名数是本实例可添加的HTTP/HTTPS域名数量，每10个域名配置限制支持1个一级域名（站点）
举例：3个域名 www.abc.com; *.abc.com; www.xyz.com，对应2个站点 abc.com和xyz.com
单实例最多可选购200个域名（20个站点）申请接入更多域名 >>
业务QPS
3000
业务QPS是无攻击状态下本实例最大可容纳HTTP/S的并发请求速率。如果正常业务QPS需要更高，请通过工单联系客服进行定制
防护端口数
50
购买量
购买数量
1
购买时长
1个月
2个月
3个月
4个月
5个月
6个月
1年
2年
自动续费

> **说明：**
> 更多信息，请参见#unique_33。

e) 确认订单并完成支付。

2. 为业务添加网站配置。

a) 登录DDoS高防（新BGP）控制台。

b) 在左侧导航栏，单击**接入管理** > **域名接入**。

c) 单击**添加网站**。

d) 在**填写网站信息**任务中，完成要防护的业务的转发配置，并单击**添加**。转发配置的描述如下。

- **功能套餐**和**实例**：要使用的高防实例
- **网站**：网站域名
- **服务器地址**：选择**源站IP**，并填写源站服务器的IP地址

> **说明：**
> 更多信息，请参见添加网站配置。

成功添加网站业务转发配置后，无需按照页面提示修改DNS解析。

3. 使用流量调度器，为业务添加防护调度规则。

   a) 登录DDoS高防（新BGP）控制台。

   b) 在左侧导航栏，单击**接入管理** > **流量调度器**。

   c) 在**通用联动**页签下，单击**添加规则**。

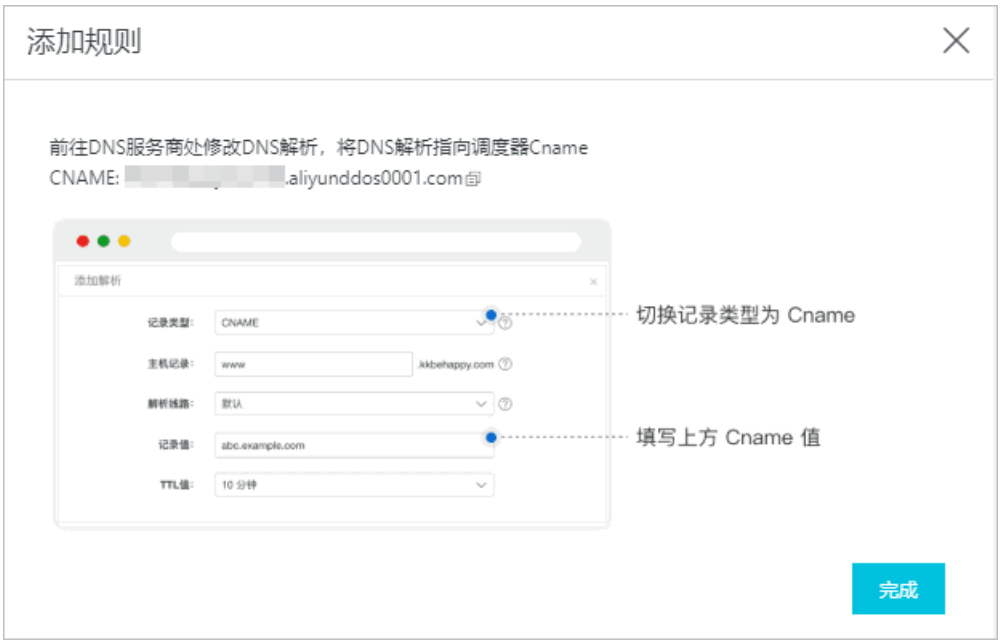
   d) 在**添加规则**页面，完成阶梯防护规则的配置，并单击**下一步**。阶梯防护规则的配置描述如下。

   - **联动场景**：**阶梯防护**
   - **DDoS高防IP**：在网站配置中使用的高防实例
   - **云资源**：业务的源站IP

说明：

更多信息，请参见#unique_35。

成功添加调度规则后，获得调度器Cname地址。



4. 更新业务域名解析。前往域名DNS服务商处修改DNS解析，使用CNAME解析，并将解析指向流量调度器Cname地址。

13 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。

14 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。

15 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。

关于访问白名单的更多操作说明，参考访问白名单。