DDoS 高防包

操作指南

产品文档

腾讯云

版权所有：腾讯云计算（北京）有限责任公司

【版权声明】

©2013-2020 腾讯云版权所有

本文档著作权归腾讯云单独所有，未经腾讯云事先书面许可，任何主体不得以任何形式复制、修改、抄袭、传播全部或部分本文档内容。

【商标声明】

腾讯云

及其它腾讯云服务相关的商标均为腾讯云计算（北京）有限责任公司及其关联公司所有。本文档涉及的第三方主体的商标，依法由权利人所有。

【服务声明】

本文档意在向客户介绍腾讯云全部或部分产品、服务的当时的整体概况，部分产品、服务的内容可能有所调整。您所购买的腾讯云产品、服务的种类、服务标准等应由您与腾讯云之间的商业合同约定，除非双方另有约定，否则，腾讯云对本文档内容不做任何明示或模式的承诺或保证。

文档目录

版权所有：腾讯云计算（北京）有限责任公司

操作指南
操作总览

最近更新时间：2019-12-23 15:28:01

您在使用 DDoS 高防包时，可能碰到诸如配置 DDoS 高防包实例、查看统计报表、查看操作日志以及设置安全事件通知等问题。本文将介绍使用 DDoS 高防包的常用操作，供您参考。

实例管理

- 查看实例详情
- 设置资源名称
- 配置弹性防护
- 更换防护对象 IP
- 解封防护 IP

防护配置

- 配置清洗阈值与防护等级
- 配置业务场景
- 管理 DDoS 高级防护策略
- 管理 CC 防护策略

统计报表

查看统计报表

操作日志

查看操作日志

安全事件通知

设置安全事件通知

版权所有：腾讯云计算（北京）有限责任公司

使用限制

最近更新时间：2019-12-23 15:28:12

防护对象限制

DDoS 高防包仅适用于腾讯云产品，包含云服务器、负载均衡、黑石物理服务器、NAT 网关等。

接入限制

DDoS 高防包仅支持绑定同一地域内的腾讯云公网 IP。

黑白名单配置限制

- DDoS 黑白 IP 名单之和最多支持添加100个 IP 地址。
- CC 黑白 IP 名单分别最多支持添加50个 IP 地址。
- CC URL 白名单最多支持添加50个 URL。

地域限制

DDoS 高防包只能绑定同一地域内的腾讯云设备，目前开放购买的地域包括：华北（北京）、华东（上海）、华南（广州）。DDoS 高防包在不同地域提供的高防能力请参考如下表格：

类型	地区	保底防护	弹性防护	最大防护能力
独享包	广州	5Gbps - 50Gbps	30Gbps - 100Gbps	100Gbps
	北京	5Gbps - 50Gbps	30Gbps - 100Gbps	100Gbps
	上海	5Gbps - 100Gbps	30Gbps - 300Gbps	300Gbps
共享包	广州	• 20Gbps • 50Gbps • 100Gbps	30Gbps - 100Gbps	100Gbps
	北京		30Gbps - 100Gbps	100Gbps
	上海		30Gbps - 300Gbps	300Gbps

版权所有：腾讯云计算（北京）有限责任公司

实例管理
查看实例详情

最近更新时间：2020-02-11 14:51:19

操作场景

您可以通过 DDoS 防护管理控制台查看所购买的 DDoS 高防包的基础信息（如实例保底防护峰值、运行状态）及实例的弹性防护配置。

操作步骤

示例：查看广州地区独享包实例“bgp-000006ee”的详细信息。

1. 登录 DDoS 防护管理控制台，在左侧导航栏中，选择【DDoS 高防包】>【资产列表】，单击【独享包】，在地区选择框中，单击【华南地区（广州）】，找到实例 ID 为“bgp-000006ee”的独享包，单击 “ID/独享包名”查看实例信息。

2. 在弹出的页面中查看如下信息：

参数说明：

- **基础信息：**
  - **服务包名**
    该 DDoS 高防包实例的名称，用于辨识与管理 DDoS 高防包实例。长度为1 - 20个字符，不限制字符类型。资源名称由用户根据实际业务需求自定义设置，具体操作请参考 设置资源名称。
  - **所在地区**
    购买 DDoS 高防包 时选择的【地域】。
  - **绑定 IP**
    该 DDoS 高防包实例所防护业务的实际 IP。
  - **保底防护峰值**
    该 DDoS 高防包实例的保底防护带宽能力，即 购买 时选择的【保底防护峰值】。若未开启弹性防护，则保底防护峰值为高防服务实例的最高防护峰值。
  - **当前状态**
    DDoS 高防包实例当前的使用状态。状态包括运行中，清洗中以及封堵中等。
  - **到期时间**
    根据 购买 时选择的【购买时长】以及具体的提支付购买订单的具体时间计算所得，精确到秒级。腾讯云会

在此时间前的前7天内，通过站内信、短信及邮件的方式向腾讯云账号的创建者以及所有协作者推送服务即将到期并提醒及时续费的信息。

- **标签**

  表示该 DDoS 高防包实例所属的标签名称，可以编辑、删除。

- **弹性防护信息：**
  - **当前状态**

    表示弹性防护是否开启。若 购买 DDoS 高防包实例 时未开启弹性防护，用户可在使用过程中自助【开启】，具体操作请参见 配置弹性防护。

  - **弹性峰值**

    开启弹性防护时，该参数项才可见，表示当前 DDoS 高防包实例的最大弹性防护能力。用户可以根据自身业务需求，随时调整弹性防护峰值，具体操作请参见 配置弹性防护。

设置资源名称

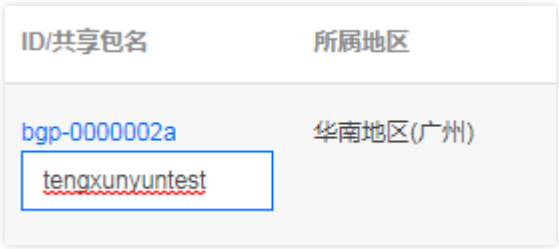
最近更新时间：2020-04-15 13:21:52

当使用多个 DDoS 高防包实例时，可通过设置【资源名称】快速辨识与管理实例。

方式一

1. 登录 DDoS 防护管理控制台，在左侧导航中，选择【DDoS 高防包】>【资产列表】，在资产列表左上方，选择地域。
2. 单击目标实例的“ID/名称”列的名称，输入名称即可。

> 说明：
> 名称长度为1 - 20个字符，不限制字符类型。



方式二

1. 登录 DDoS 防护管理控制台，在左侧导航中，选择【DDoS 高防包】>【资产列表】，在资产列表左上方，选择地域。
2. 在下方实例列表中，单击目标实例的“ID/名称”列的实例名称，进入实例的基础信息页面。

3. 在实例的基础信息页面中，单击基础信息右侧的【编辑】，输入或修改名称，并单击【确定】即可。

说明：
名称长度为1 - 20个字符，不限制字符类型。

配置弹性防护

最近更新时间：2020-03-18 09:42:24

DDoS 高防包实例启用弹性防护后，当攻击流量峰值超出保底防护峰值时，DDoS 高防包会根据用户设置的弹性防护峰值继续进行防护。
若 购买 DDoS 高防包实例 时，未开启弹性防护，用户可在使用过程中自助开启。当天未触发弹性防护，不产生额外费用。在触发弹性防护（攻击峰值超过保底防护峰值）时，取当天实际产生的最高攻击峰值所对应区间进行 计费，账单次日生成。用户可根据实际业务情况实时更改 DDoS 高防包实例的弹性防护峰值。

开启弹性防护

> 说明：
> 若 购买 DDoS 高防包实例 时未开启弹性防护，用户可在使用过程中开启，并以历史最高攻击流量为参考，选择略高于历史最高峰值的弹性防护峰值，以便足够防御大流量攻击，避免超过防护峰值而引起的 IP 封堵。

1. 登录 DDoS 防护管理控制台，选择【DDoS 高防包】>【资产列表】，在目标实例所在行，单击【开启弹性防护】。
2. 在【开启弹性防护】对话框中，选择合适的【弹性防护峰值】。

3. 单击【确定提交】。

更改弹性防护峰值

1. 登录 DDoS 防护管理控制台，选择【DDoS 高防包】>【资产列表】，单击目的实例，进入实例的基础信息界面。
2. 找到"弹性防护"部分，单击【防护峰值】右侧的【更改】。

3. 在【更改弹性防护】对话框中，选择合适的【弹性防护峰值】。

说明：

- 弹性防护峰值支持调升调降，不同地域支持的防护能力不同，弹性防护峰值的具体取值范围请参考 使用限制。
- 弹性防护峰值修改后立即生效。

4. 单击【确定提交】。

关闭弹性防护

> 说明：
> 关闭弹性防护后，最大防护峰值降为保底防护峰值，请确保是否满足实际需求再执行此操作。

1. 登录 DDoS 防护管理控制台，选择【DDoS 高防包】>【资产列表】，在目标实例所在行，单击【关闭弹性防护】。
2. 在【关闭弹性防护】对话框中，单击【确定提交】。

管理防护对象 IP

最近更新时间：2020-02-12 10:38:13

操作场景

DDoS 高防包为腾讯云公网 IP 提供更高的 DDoS 防护能力，可支持防护 CVM、CLB、NAT、WAF 等产品和服务。用户根据实际业务需求，可以更换已绑定到 DDoS 高防包实例的防护对象 IP，也可以一键解绑已绑定到 DDoS 高防包的防护对象 IP。

前提条件

在更换、或解绑防护对象 IP，您需要成功 购买 DDoS 高防包实例 并已为其 绑定防护对象 IP。

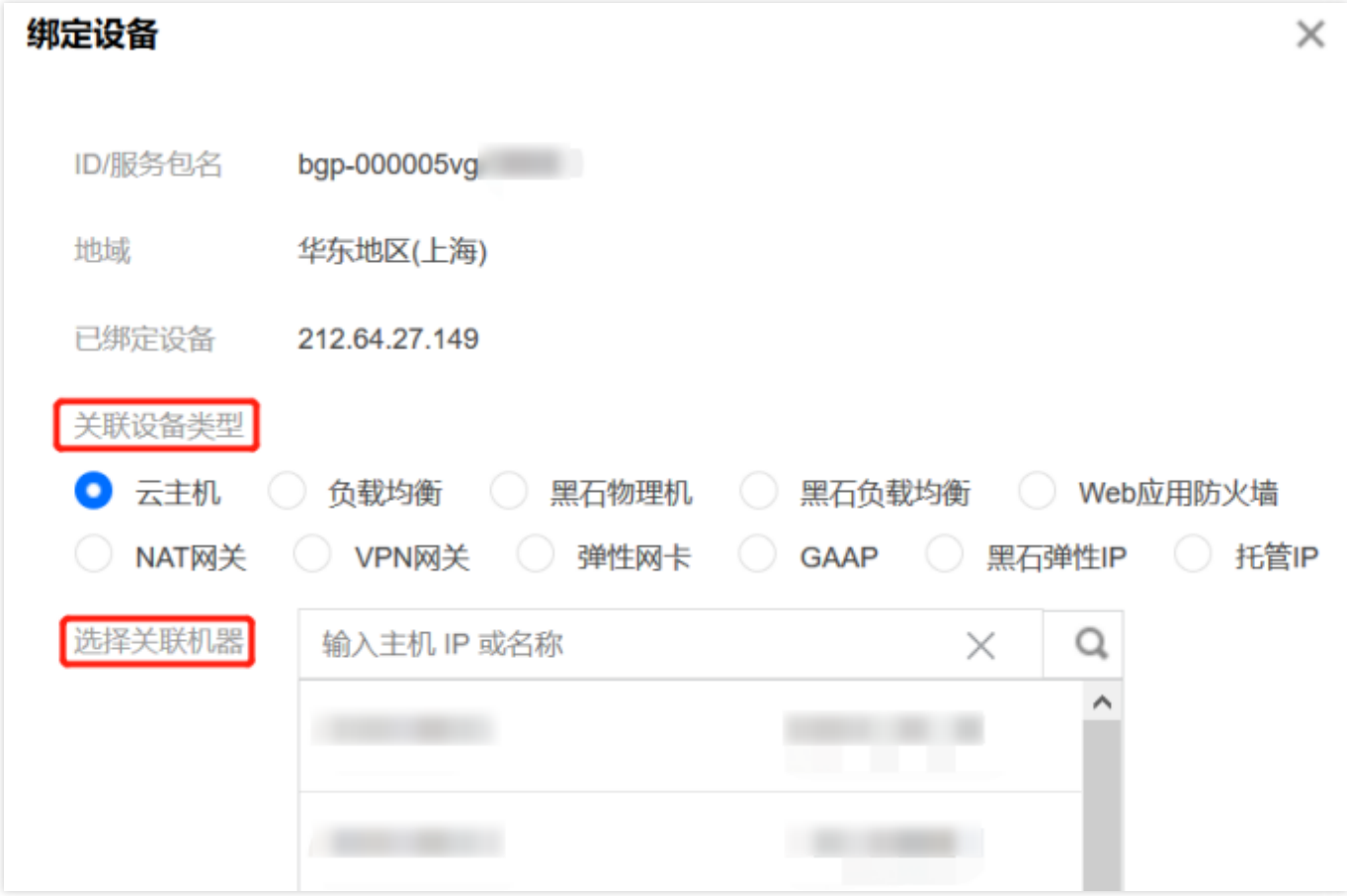
操作步骤

更换防护对象 IP

1. 登录 DDoS 防护管理控制台，在左侧导航中，选择【DDoS 高防包】>【资产列表】，在页面上方，选择地域。
   - 若您的 DDoS 高防包实例是独享包，则选择【独享包】页签。
   - 若您的 DDoS 高防包实例是共享包，则选择【共享包】页签。
2. 单击目标 DDoS 高防包实例所在行的【更换设备】。
3. 在【绑定设备】页面，根据实际防护需求选择【关联设备类型】与【选择关联机器】。

版权所有：腾讯云计算（北京）有限责任公司

- 若您的 DDoS 高防包实例是独享包，仅支持绑定一个关联机器。



- 若您的 DDoS 高防包实例是共享包，【关联设备类型】与【选择关联机器】均允许多选，【选择关联机器】数量不得超过 购买 DDoS 高防包实例 时设置的【IP 数量】。

4. 单击【确定】。

解绑防护对象 IP

1. 登录 DDoS 防护管理控制台，在左侧导航中，选择【DDoS 高防包】>【资产列表】，在页面上方，选择地域。
   - 若您的 DDoS 高防包实例是独享包，则选择【独享包】页签。
   - 若您的 DDoS 高防包实例是共享包，则选择【共享包】页签。
2. 单击目标 DDoS 高防包实例所在行的【更多】>【解绑】，在弹出的会话框中，单击【确定】即可。

解封防护 IP

最近更新时间：2020-02-11 14:51:59

DDoS 高防包对进入封堵状态的防护 IP 提供解封的功能，您可以登录 DDoS 防护管理控制台 进行自助解封操作。

自助解封次数

使用 DDoS 高防包的用户每天将拥有**三次**自助解封机会，当天超过三次后将无法进行解封操作。系统将在每天零点时重置自助解封次数，当天未使用的解封次数不会累计到次日。

说明：

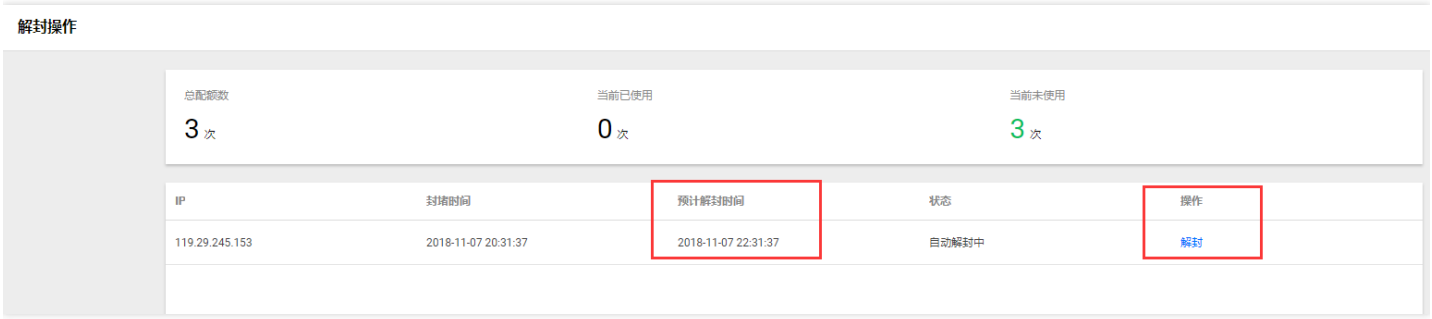
- 由于解封涉及腾讯云大禹后台系统的风控管理策略，解封可能失败（解封失败不会扣减您的剩余解封次数），请您耐心等待一段时间后再次尝试。
- 在执行解封操作前，建议您先查看预计解封时间，预计解封时间受到部分因素影响，可能会推后。如果您可以接受预计时间，则无需手动操作。
- 当天自助解封配额为0时，建议提升保底防护能力或弹性防护能力，以便足够防御大流量攻击，避免被持续封堵。

自助解封操作

登录 DDoS 防护管理控制台，选择【自助解封】>【解封操作】，找到状态为自动解封中的防护 IP，单击【操作】列中的【解封】。在【解除封堵】对话框中，单击【确定】。

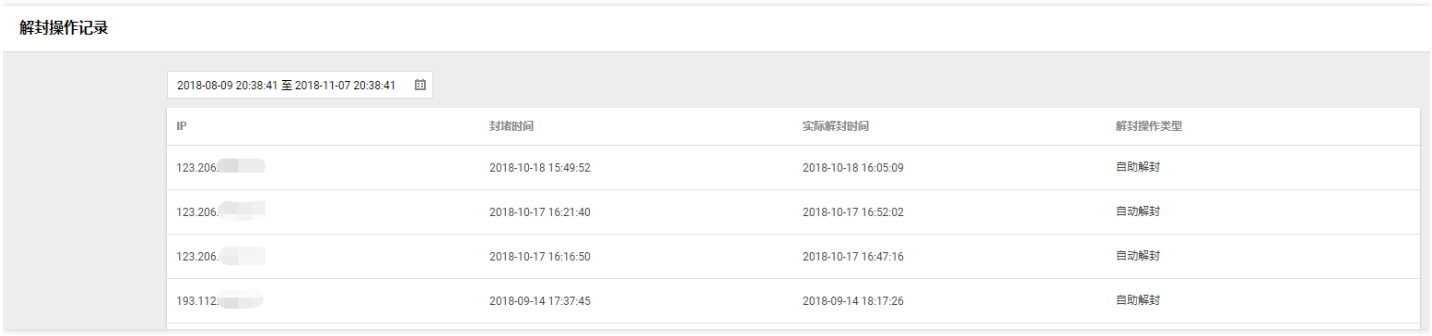
- 如果解封失败，您会收到解封失败提示信息，请您耐心等待一段时间后再尝试。
- 如果收到解封成功提示信息，则表示封堵状态已成功解除，您可以刷新页面确认该防护 IP 是否已恢复运行中状态。

版权所有：腾讯云计算（北京）有限责任公司



解封操作记录

登录 DDoS 防护管理控制台，选择【自助解封】>【解封操作记录】，根据时间范围筛选，可查看所有解封操作记录，包括自动解封、手工自助解封等操作记录。



防护配置
配置清洗阈值与防护等级

最近更新时间：2020-02-12 10:37:10

应用场景

DDoS 高防包服务提供防护策略调整功能，针对 DDoS 攻击提供三种防护等级供您选择，各个防护等级的具体防护操作如下：

防护等级	防护操作	描述
宽松	• 过滤明确攻击特征的 SYN、ACK 数据包。 • 过滤不符合协议规范的 TCP、UDP、ICMP 数据包。 • 过滤具有明确攻击特征的 UDP 数据包。	• 清洗策略相对宽松，仅对具有明确攻击特征的攻击包进行防护。 • 建议在怀疑有误杀时启用，遇到复杂攻击时可能会有攻击透传。
正常	• 过滤明确攻击特征的 SYN、ACK 数据包。 • 过滤不符合协议规范的 TCP、UDP、ICMP 数据包。 • 过滤具有明确攻击特征的 UDP 数据包。 • 过滤常见基于 UDP 的攻击数据包。 • 对部分访问源 IP 进行主动验证。	• 清洗策略适配绝大多数业务，可有效防护常见攻击。 • 默认为正常模式。
严格	• 过滤明确攻击特征的 SYN、ACK 数据包。 • 过滤不符合协议规范的 TCP、UDP、ICMP 数据包。 • 过滤具有明确攻击特征的 UDP 数据包。 • 过滤常见基于 UDP 的攻击数据包。 • 对部分访问源 IP 进行主动验证。 • 过滤 ICMP 攻击包。 • 过滤常见的 UDP 攻击数据包。	清洗策略相对严格，建议在正常模式出现攻击透传时使用。

版权所有：腾讯云计算（北京）有限责任公司

	• UDP 数据包严格检查。	

说明：
如果您的业务需要使用 UDP，建议您联系 腾讯云技术支持 进行策略定制，以免严格模式影响业务流程。

默认情况下，您所购买的 DDoS 高防包实例采用正常防护等级，您可以根据实际业务情况自由调整 DDoS 防护等级。同时，您还可以自定义设置清洗阈值，当攻击流量超过设置的阈值时，将启动清洗。

配置示例

下面以配置华南地区（广州）的实例“bgp-000006ee”为例，进行配置说明：

1. 登录 DDoS 防护管理控制台，在左侧导航栏中，选择【DDoS 高防包】>【资产列表】，单击【独享包】，在地区选择框中，单击【华南地区（广州）】，找到实例 ID 为“bgp-000006ee”的独享包，在右侧操作项中，单击【防护配置】进行配置。
2. 在弹出的 DDoS 防护配置的页面中，开启【防护状态】，进行清洗阈值、防护等级的设置。

> 注意：
> 仅当“防护状态”为  状态时，下面配置项才可见。若手动将防护状态关闭，则配置项隐藏且配置不生效，重新开启后，配置项可见且保持原有的配置数据。

配置参数说明：

- **防护状态**
  默认开启，您可根据实际业务需求开启或关闭防护。关闭防护时，可进行关闭时长的设置，目前只能临时关闭防护1 - 6小时，超过所设置的时长或当攻击流量超过100wpps或2Gbps时，DDoS 高防包将自动开启防护。
- **清洗阈值**
  - 清洗阈值是高防产品启动清洗动作的阈值。当流量小于阈值时，即使检测到攻击也不会进行清洗操作。
  - 默认在开启“防护状态”的情况下，业务刚接入的 DDoS 高防包实例的清洗阈值采用默认值，并随着接入业务流量的变化规律，系统自动学习形成一个基线值。您可以根据实际业务情况自由设置清洗阈值。

    > 说明：
    > 若明确该清洗阈值，可进行自定义设置。若无法明确该清洗阈值，DDoS 防护系统将根据 AI 算法自动学习并生成一套专属的默认阈值。

- **防护等级**
  默认在开启“防护状态”的情况下，业务刚接入的 DDoS 高防包实例采用正常防护等级，您可以根据实际业务防护需求自由调整 DDoS 防护等级。
- **其他配置项**
  - **业务场景**
    您可以根据实际业务需求，从已创建的业务场景中选择一个匹配的业务场景，支持修改。当选择某一个业务场景后，对应的“高级策略”会自动匹配该业务场景生成的策略。请参见 配置业务场景 进行业务场景创建。
  - **高级策略**
    您可根据业务防护特性，从已创建的高级策略中选择一个匹配的高级策略，支持修改。请参见 管理 DDoS 高级防护策略 进行高级防护策略创建。
  - **DDoS 攻击告警阈值**
    新增 DDoS 攻击告警阈值配置功能。若检测的指标超过您设定的阈值，将触发告警，并向您推送攻击告警信息。请参见 配置攻击告警阈值 进行告警指标设置。
  - **TCP 业务 AI 增强防护**
    针对四层 TCP 业务，DDoS 高防包提供 TCP 业务 AI 增强防护功能，开启后，通过 AI 模型日常业务特征的自学习，能够自动识别业务流量与攻击流量，有效防护线上的四层 CC 攻击。

    > 说明：

目前 TCP 业务 AI 增强防护功能仅对白名单开放。

配置业务场景

最近更新时间：2020-02-11 14:50:47

应用场景

DDoS 高防包支持自定义 DDoS 高级防护策略，用户可以根据业务特点或攻击行为针对性地设置防护策略。通常每个高防包实例最多绑定一个 DDoS 高级防护策略。当用户的账号下拥有多个高防包实例时，最多拥有5个 DDoS 高级防护策略可供选择。
为满足实际业务需要或应对不断变化的攻击手法，用户可能需要不断优化策略配置。为简化 DDoS 精细化防护管理，DDoS 高防包提供业务场景设置功能，通过创建业务应用场景，后台收集、识别并自动生成高级防护策略，实现灵活的配置或维护策略。

创建业务场景

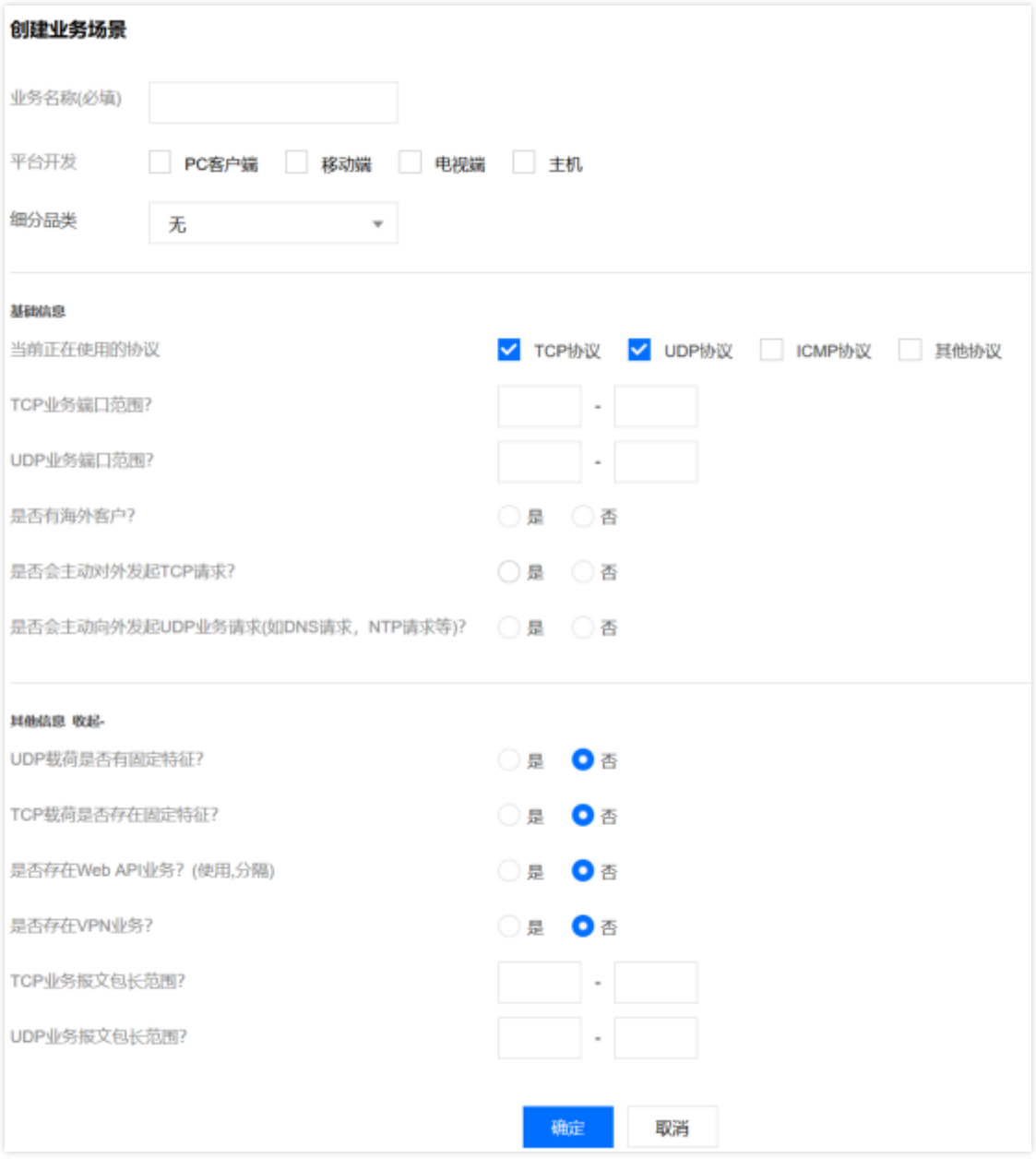
- **方法一：**
  若用户所购 DDoS 高防包实例未配置业务场景，登录 DDoS 防护管理控制台，在左侧导航中选择【DDoS 高防包】>【防护配置】，会弹出如下图所示的提示信息，单击【去创建】，进行业务场景的创建。

> 说明：
> 最多支持创建5个业务场景。

- **方法二：**

1. 登录 DDoS 防护管理控制台，在左侧导航中选择【BGP 高防包】>【防护配置】，在防护配置页面中，选择【DDoS 高级防护策略】>【创建业务场景】。

2. 在【创建业务场景】页面，根据实际业务特点，输入以下参数，单击【确定】完成1个业务场景的设置。



- **业务名称：**必填项，输入业务名称，长度为1 - 32个字符，不限制字符类型。

- **平台开发：**勾选平台开发对应的类型。可供选择的有 PC 客户端、移动端、电视端和主机。
- **细分品类：**选择业务所属类型。可供选择的有游戏、应用、网站或其他类型。
- **基础信息：**
  - **当前正在使用的协议：**勾选正在使用的协议，支持可选的协议有 ICMP、TCP、UDP 和其他协议（指除了 ICMP、TCP、UDP 以外的协议）。

    说明：
    当勾选 TCP、UDP协议时，则需要输入 TCP/ UDP 业务端口范围，可填范围为1 - 65535，同时其他信息区域会弹出 TCP/ UDP 业务报文包长范围配置，该配置为选填项，可填的报文包长范围为0 - 1500。

  - **是否有海外客户**？
    勾选【是】或【否】，对应生成策略的配置项为关闭 / 开启【拒绝海外流量】。
  - **是否会主动对外发起 TCP 请求**？
    勾选【是】或【否】。选择【是】，需要填写主动对外发起 TCP 请求的端口。存在多个请求业务端口时，全部填入并用英文“,”分隔。
  - **是否会主动向外发起 UDP 业务请求（DNS 请求，NTP 请求等）**？
    勾选【是】或【否】。选择【是】，需要填写主动对外发起 UDP 业务请求的端口。存在多个请求业务端口时，全部填入并用英文“,”分隔。
- **其他信息**：（单击【展开+】即可选择对应参数）
  - **UDP载荷是否有固定特征**？
    勾选【是】或【否】。默认【否】，当选择【是】时，需要填写 UDP 载荷特征内容。
  - **TCP载荷是否存在固定特征**？
    勾选【是】或【否】。默认【否】，当选择【是】时，需要填写 TCP 载荷特征内容。
  - **是否存在 Web API 业务**？
    勾选【是】或【否】。默认【否】，当选择【是】时，需要填写 API 业务 URL。存在多个 API 业务 URL 时，全部填入并用英文“,”分隔。
  - **是否存在 VPN 业务**？
    勾选【是】或【否】。默认【否】，若选择【是】时，则不会禁用“其他协议”。

    说明：
    在“当前正在使用的协议”、“是否存在 VPN 业务”两项参数中，只要存在条件之一即勾选“其他协议”或选择“【是】存在 VPN 业务”，则不会禁用“其他协议”。

版权所有：腾讯云计算（北京）有限责任公司

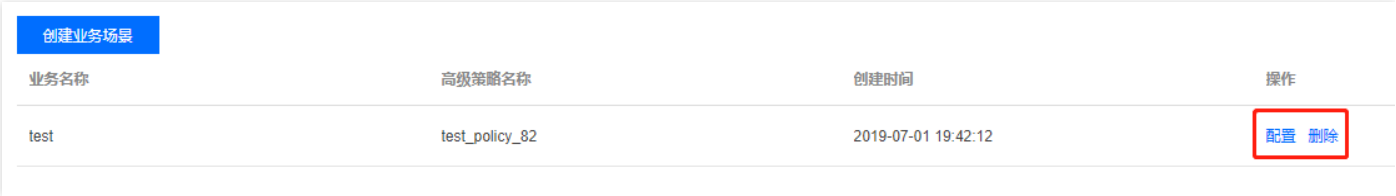
3. 后台对用户创建的业务场景进行分析后，自动生成1条以“业务场景名称_ policy_序号”（如“test_policy_1”）命名的高级防护策略，用户再根据实际特殊业务防护需求，自主配置或调整该条防护策略。

> 注意：
>
> - 在用户只拥有一个 DDoS 高防包实例的情况下，若只创建一个业务场景，则自动将对应生成的高级防护策略绑定到当前实例中。
> - 当对业务场景信息修改后，对应生成的高级防护策略会自动同步相关配置项信息。若对该条高级防护策略进行调整，则不会同步到对应的业务场景信息。

修改和删除业务场景

1. 登录 DDoS 防护管理控制台，在左侧导航中选择【DDoS 高防包】>【防护配置】。
2. 在【DDoS 高级防护策略】页面，找到目的业务场景，单击【配置】或【删除】，进行修改或者删除。

> 说明：
> 当对目的业务场景进行删除操作，则对应的高级防护策略也将删除。



若需要了解更多信息，请参见 管理 DDoS 高级防护策略。

管理 DDoS 高级防护策略

最近更新时间：2020-02-11 14:46:28

DDoS 高防包提供面向 DDoS 攻击的高级防护策略功能，用户可针对自身业务防护需求对 DDoS 防护策略进行调整和优化。通过黑白名单、禁用协议、禁用端口、报文特征过滤策略、连接耗尽防护、水印防护等功能，为业务提供针对性防护。

配置项简介

配置项	功能简介	生效时间
黑白名单	基于 IP 地址级别的防护。 • 白名单中的 IP，访问时将被直接放行，不经过任何防护策略过滤。 • 黑名单中的 IP，访问时将会被直接阻断。	当被防护的 IP 处于被攻击状态时生效。
禁用协议	可禁用业务不使用的协议。 当检测到攻击行为时，大禹高防集群会清洗掉该协议的流量。	当被防护的 IP 处于被攻击状态时生效。
禁用端口	可禁用业务不使用的端口。 当检测到攻击行为时，大禹高防集群会清洗掉该端口的流量。	当被防护的 IP 处于被攻击状态时生效。
报文过滤特征	可以针对业务报文特征或攻击报文特征，将协议、端口范围、包长范围、是否检测载荷、偏移量、检查深度、是否包括特征字符串等条件进行组合，设定策略动作。 当检测到报文匹配到策略条件时，可以执行直接转发、丢弃、拉黑源 IP 或断开连接等操作。	当被防护的 IP 处于被攻击状态时生效。
限速	基于目的IP的防护，对访问协议进行限速控制。	当被防护的 IP 处于被攻击状态时生效。
拒绝海外流量	可拒绝来自中国（大陆地区及港澳台）以外的 TCP 流量请求。	当被防护的 IP 处于被攻击状态时生效。

版权所有：腾讯云计算（北京）有限责任公司

配置项	功能简介	生效时间
空连接防护	应对空连接攻击。	当被防护的 IP 处于被攻击状态时生效。
连接耗尽防护	基于 IP 地址的防护，对于接入高防包的防护 IP 的连接速度、包长度等参数进行限制，实现缓解小流量的连接型攻击的防护功能。	当被防护的 IP 处于被攻击状态时生效。
异常连接检测	当一个源 IP 接收到的一个 TCP 连接符合所配置的参数特征时，将判断为异常连接，同时当该源 IP 所接收到的异常连接数超过所设置的最大异常连接数时，会被加入黑名单一定时间，禁止被访问。	当被防护的 IP 处于被攻击状态时生效。
水印防护	支持 UDP 和 TCP 报文，在配置的端口范围内，其载荷进行水印检测和剥离。通过接入水印防护，高效全面防护 4 层 CC 攻击，如模拟业务报文攻击和重放攻击等。 • 业务端和腾讯云大禹安全防护系统端共享水印算法和密钥。 • 客户端每个发出的报文都嵌入了水印特征，而攻击报文却无水印特征。 • 大禹安全防护系统将甄别出攻击报文并将其丢弃。	当被防护的 IP 处于被攻击状态时生效。

添加新策略

> 注意：
> 高级安全防护策略功能具有一定专业性，建议有相关经验的用户在阅读以下操作指南后根据实际情况进行配置。

登录 DDoS 防护管理控制台，选择【DDoS 高防包】>【防护配置】。在【DDoS 高级防护策略】页签，单击【添加新策略】。根据实际业务需求设置以下参数，单击【确定】。

- **策略名称**
  输入策略名称，长度为1 - 32个字符，不限制字符类型。

- **黑白名单**
  - 若需设置黑名单：单击【添加】，选择【黑名单】，填写需要拦截的 IP，存在多个 IP 时可全部填入并用回车分隔多个 IP，单击【确定】。
  - 若需设置白名单：单击【添加】，选择【白名单】，填写需要放行的 IP，存在多个 IP 时可全部填入并用回车分隔多个 IP，单击【确定】。

> 说明：
> 黑白 IP 名单之和最多支持添加100个 IP，批量添加的 IP 数不允许超过当前配额。

- **禁用协议**
  选择需要禁用的协议。

- **禁用端口**
  选择协议和端口类型，然后填写对应需要禁用的端口。若某条记录中仅需禁用一个端口，则开始端口号和结束端口号填写相同值即可。单击列表下方的【增加】可新增多条记录。协议包括TCP、UDP两种协议，端口类型包括目的端口、源端口、目的端口和源端口三种类型。

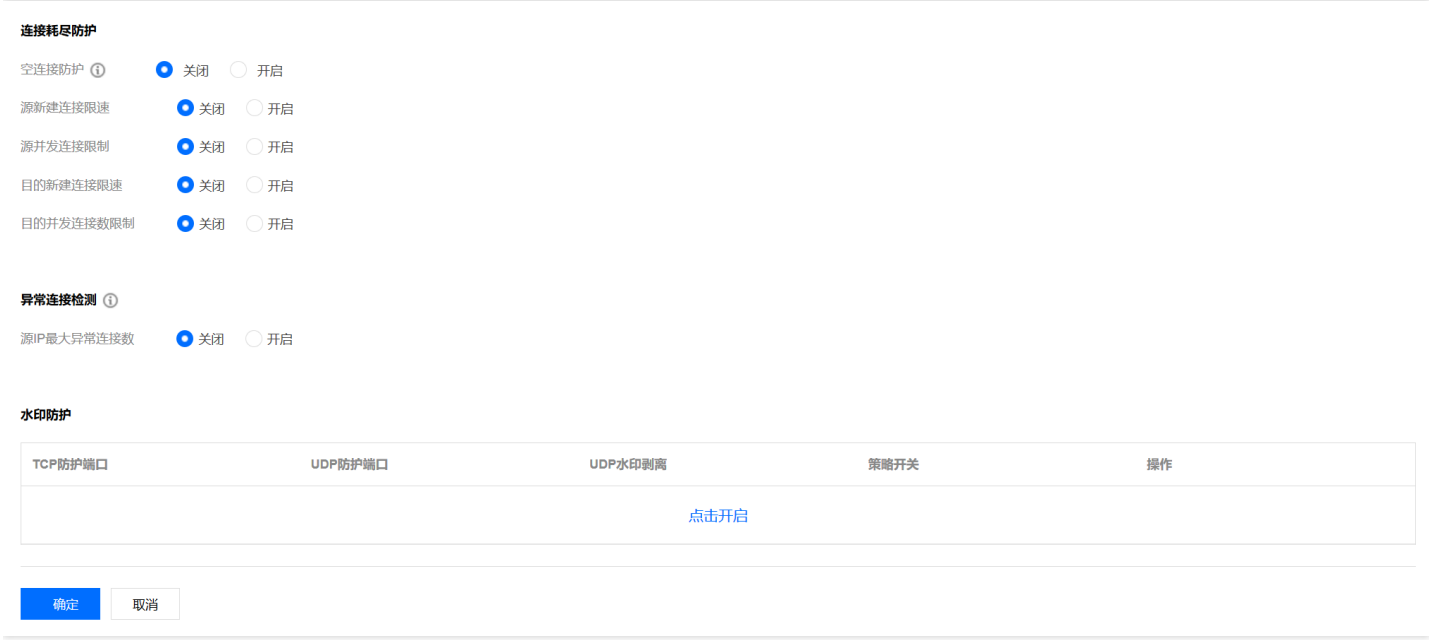
- **报文过滤特征**
  支持将协议、端口范围、包长范围、是否检测载荷、偏移量、检查深度、是否包括特征字符串等条件进行组合，设定策略动作且即刻生效。

  说明：
  - 偏移量：表示报文内容中开始匹配的特征的位置。
  - 检查深度：配合偏移量使用，表示从偏移量设定的位置开始向后匹配的报文内容长度。
  - 策略：
    - “丢弃报文”表示丢弃匹配该报文过滤特征的数据包。
    - “丢弃且拉黑源 IP”表示丢弃匹配该报文过滤特征的数据包并将源 IP 临时拉黑一段时间。
    - “丢弃且断开连接”表示丢弃匹配该报文过滤特征的数据包并断开 TCP 连接。
    - “丢弃，断开连接且拉黑源 IP”表示丢弃匹配该报文过滤特征的数据包，同时断开 TCP 连接并将源 IP 临时拉黑一段时间。
    - “直接转发”表示直接转发匹配该报文过滤特征的数据包。

版权所有：腾讯云计算（北京）有限责任公司

- **限速**
  单击【添加】，选择需要限速的协议，设置限速阈值。支持限速的可选协议有 ICMP、TCP、UDP 和其他协议，这里的其他协议指除了 ICMP、TCP、UDP 以外的协议。

- **拒绝海外流量**
  勾选开启或关闭。DDoS 高防包的防护引擎内置海外 IP 库，开启拒绝海外流量后将基于该 IP 库对来源进行判断并执行阻断。勾选【开启】时，需处于被攻击状态才生效。勾选【关闭】时即刻生效。



- **连接耗尽防护**
  - **空连接防护**：勾选开启或关闭。勾选【开启】时，需处于被攻击状态才生效。由于基于 TCP 代理原理实现，对于业务的首次访问体验可能会有影响。
  - **源新建连接限速**：勾选开启或关闭。勾选【开启】时，设置抑制速率（单位：个/秒），可填范围 0-∞。表示单一源IP每秒新建连接速率，超过限制的新建连接将被丢弃。
  - **源并发连接限速**：勾选开启或关闭。勾选【开启】时，设置抑制数（单位：个），可填范围 0-∞。表示单一源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**：勾选开启或关闭。勾选【开启】时，设置抑制速率（单位：个/秒），可填范围 0-∞。表示目的IP每秒最大新建连接速率，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**：勾选开启或关闭。勾选【开启】时，设置抑制数（单位：个），可填范围 0-∞。表示目的IP 最大并发连接数，超过限制的并发连接将被丢弃。由于防护设备为集群化部署，并发连接限速存在一定误差。
- **异常连接检测**

- **源 IP 最大异常连接数**：单击【开启】，填写源 IP 最大异常连接数量，可填范围 0-∞（单位：个）。表示当一个源 IP 符合异常连接行为识别的连接数，超过所指定阈值时，会被认为是异常攻击源，在一定时间内被限制访问。

  > 说明：
  > 只有开启源 IP 最大异常连接数，以下参数才能进行配置。

- **Syn 报文占比检测**：勾选开启或关闭。勾选【开启】时，设置 Syn 报文占比值，可填范围 0-100。表示当一个 TCP 连接中的 Syn 报文数与 Ack 报文数的比例超过所配置阈值时，会被识别为一个异常连接。
- **Syn 报文数检测**：勾选开启或关闭。勾选【开启】时，设置最大报文数，可填范围 0-65535。表示当一个 TCP 连接中的 Syn 报文数超过所配置最大报文数时，会被识别为异常连接。
- **连接超时检测**：勾选开启或关闭。勾选【开启】时，设置检测周期（单位：秒），可填范围 0-65535。表示一个 TCP 连接创建后在所设置的时间内没有任何报文传输则判断为异常连接。
- **异常空连接检测**：勾选开启或关闭。表示一个 TCP 连接创建后没有任何带有载荷的报文传输则判断为异常连接。

- **水印防护**
  单击【开启】进行水印防护配置。填写指定的 TCP 协议防护端口和 UDP 协议防护端口，单击【确定】水印防护

功能即刻开启。添加 DDoS 高级防护策略后，自动产生一条密钥信息，需要完成线下客户端接入水印配置。

- **TCP 协议防护端口、UDP 协议防护端口**
  TCP/UDP 防护端口最多可以配置5个端口段；不同端口段不可以互相重合；起止端口号相同则认为是一个端口；TCP 或 UDP 协议端口段中需要至少配置一条。

绑定与解绑资源

登录 DDoS 防护管理控制台，选择【DDoS 高防包】>【防护配置】。在【DDoS 高级防护策略】页签，单击目标策略所在行的【绑定资源】。

- 绑定资源：在弹出的【绑定资源】对话框中，根据实际业务需求勾选一个或多个资源，单击【确定】。
- 解绑资源：在弹出的【绑定资源】对话框中，根据实际业务需求单击【已选择】区域中已选资源右侧的×，单击【确定】。

客户端接入水印

登录 DDoS 防护管理控制台，选择【DDoS 高防包】>【防护配置】。在【DDoS 高级防护策略】页签，单击目标策略所在行的【水印客户端文件下载】，线下完成客户端的接入。

添加、删除或停用/启用水印密钥

登录 DDoS 防护管理控制台，选择【DDoS 高防包】>【防护配置】。在【DDoS 高级防护策略】页签，单击目标策略所在行的【水印密钥配置】。

- **添加密钥**：在弹出的【密钥信息】对话框中，单击【添加密钥】即刻生成新密钥。
- **停用/启用密钥**：支持对密钥进行停用或启用操作。在弹出的【密钥信息】对话框中，单击目的密钥所在行的【停用】；如需重新开启则单击【启用】即可。
- **删除密钥**：只能对已停用的密钥进行删除。在弹出的【密钥信息】对话框中，单击目的密钥所在行的【删除】即可。

> 说明：
> 最多可存在2个密钥，如果需要添加新密钥，请先删掉其中一个旧密钥；当仅有一个密钥生效时，不可将其停用或删除。

版权所有：腾讯云计算（北京）有限责任公司

配置策略

登录 DDoS 防护管理控制台，选择【DDoS 高防包】>【防护配置】。在【DDoS 高级防护策略】页签，单击目标策略所在行的【配置】。根据实际业务需求更新以下参数，单击【确定】保存修改。

> 说明：
> 当目的策略是以"业务场景名称 _ policy_ 序号"形式命名的，则不能对策略名称进行修改。

- 策略名称
- 黑白名单
- 禁用协议
- 禁用端口
- 报文过滤特征
- 拒绝海外流量
- 连接耗尽防护
- 异常连接检测
- 水印防护

删除策略

> 说明：

- 未绑定资源的策略可直接删除，已绑定资源的策略需要先将所有资源解绑再执行删除操作；策略删除后不可恢复，请谨慎操作。
- **不能对根据用户创建的业务场景自动生成的高级防护策略进行删除操作。**

登录 DDoS 防护管理控制台，选择【DDoS 高防包】>【防护配置】。在【DDoS 高级防护策略】页签，单击目标策略所在行的【删除】。在弹出的对话框中，单击【确定】。

配置 CC 防护策略

最近更新时间：2019-12-30 19:27:52

操作场景

DDoS 高防包支持 CC 防护功能，当高防包统计的 HTTP 请求量超过设定的【http 请求数阈值】时，自动触发 CC 防护。同时，DDoS 高防包还支持 URL 白名单、IP 白名单和 IP 黑名单策略：

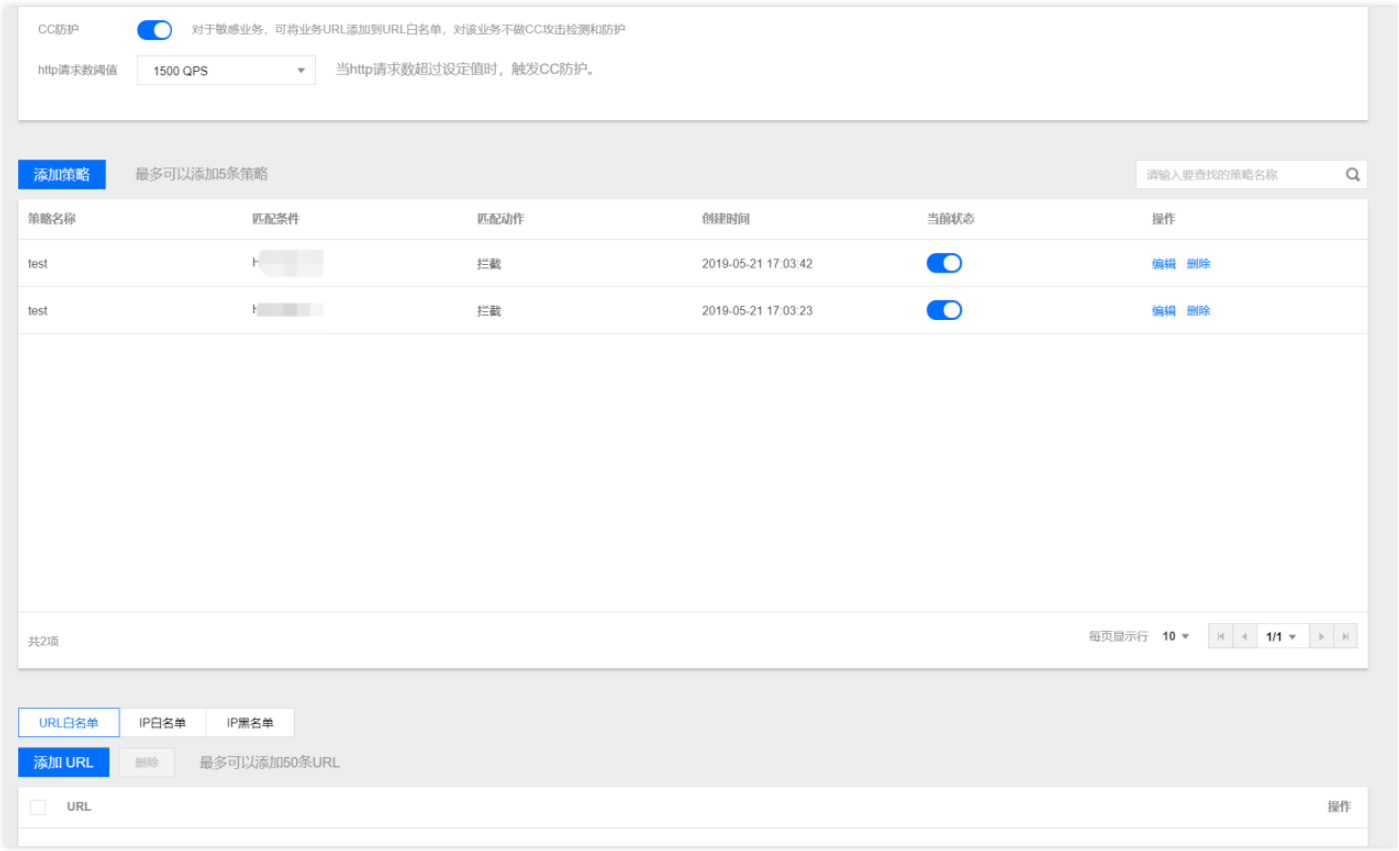
- 白名单中的 URL，其访问请求将无需执行 CC 攻击检测，直接被放行。
- 白名单中 IP，其 HTTP 访问请求将无需执行 CC 攻击检测，直接被放行。
- 黑名单中 IP，其 HTTP 访问请求将直接被拒绝。

用户可根据业务特点和防护需求，自定义防护策略实现更精准的 CC 攻击拦截。

操作步骤

1. 登录 DDoS 防护管理控制台，选择【DDoS 高防包】>【防护配置】，在【CC 防护】页签，选择目标地域和高防包实例，进行 CC 防护配置。

版权所有：腾讯云计算（北京）有限责任公司



2. 单击【CC 防护】右侧的  开启 CC 防护。

> 说明：
>
> - CC 防护默认关闭。
> - 开启 CC 防护后，才可设置 HTTP 请求数阈值、自定义 CC 防护策略以及黑白名单。

3. 单击【http 请求数阈值】右侧的下拉框选择合适的阈值。

4. 单击【添加访问控制策略】，在【添加访问控制策略】弹出框中，根据实际业务需求设置以下参数，单击【确定】完成配置。

说明：

- **仅在该高防包正在被攻击状态时，自定义策略才会生效。**
- **匹配模式下**，每个自定义策略最多可以设置**4**个策略条件进行特征控制，且多个条件之间是"与"的关系，需要所有条件全部匹配策略才生效。
- **限速模式下**，每个自定义策略只允许设置**1**条策略条件。

- **策略名称**
  输入策略名称，长度为1 - 20字符，不限制字符类型。
- **模式**
  - 匹配模式：匹配到 HTTP 对应字段头的请求，执行拦截或人机识别操作。
  - 限速模式：对源 IP 访问进行限速处理。
- **策略**
  - 当选择【匹配模式】时，支持从 HTTP 报文的 host 参数、CGI 参数、Referer 和 User-Agent 等多个特征进行组合，组合逻辑包括包含、不包含和等于。最多可以设置4个策略条件进行特征控制，字段描述如下：

匹配字段	字段描述	适用的逻辑符
host	访问请求的域名。	包含、不包含、等

		于。
CGI	访问请求的 URL 地址。	包含、不包含、等于。
Referer	访问请求的来源网址，表示该访问请求是从哪个页面跳转产生的。	包含、不包含、等于。
User-Agent	发起访问请求的客户端浏览器标识等相关信息。	包含、不包含、等于。

- 当选择【限速模式】时，对每个源 IP 访问进行限速处理。只允许设置1个策略条件。

5. 单击【URL 白名单】、【IP 白名单】或【IP 黑名单】页签，进行黑白名单配置，支持添加、删除。

> 说明：
> DDoS 高防包添加 URL 白名单时，可以带 HTTP 协议头信息，也可以不带 HTTP 协议头信息，但 DDoS 高防包仅支持 HTTP 协议。例如可以填写 `http://test.com/index.php` 或 `www.test.com/index.php`。

配置智能调度

最近更新时间：2020-03-23 11:38:55

应用场景

一般每个账号下可能拥有多个高防实例，且每个高防实例至少拥有一条高防线路，因此每个账号下可能会存在多条高防线路。当将业务添加至高防实例进行防护后，表示您已经为该业务配置一条高防线路作为防护线路。若您的业务配置存在多条高防线路作为防护线路，您需要考虑该业务流量的最佳调度方式，即如何将业务流量调度到最优的高防线路进行防护，保证业务访问速度和高可用性。
目前 DDoS 防护（大禹）服务提供优先级方式的 CNAME 智能调度功能，您可以根据实际需要，勾选高防实例并设置高防线路的优先级。

> 说明：
> 支持设置解析的高防实例有 DDoS 高防包、DDoS 高防 IP 和 DDoS 高防 IP 专业版，其中 DDoS 高防包包括独享包和共享包。

优先级调度方式

指针对所有的 DNS 请求均以优先级最高的高防线路进行响应，即所有访问流量被调度至当前优先级最高的高防线路。您可以编辑高防线路的优先级，默认优先级为100，优先级的值越小，则表示该高防线路优先级越高。具体调度规则如下：

- 如果业务配置的高防实例包含多条不同高防线路，且优先级相同时，则按照 DNS 请求的运营商来源进行响应。当其中某条高防线路遭遇封堵后，将按照 BGP > 电信 > 联通 > 移动 > 境外（包括中国香港、中国台湾）的线路顺序进行调度。
- 如果同一优先级的高防线路均遭遇封堵后，访问流量将自动调度到当前可用的优先级次高的高防线路。

> 注意：
> 若当前无次高优先级的高防线路可用，则无法进行自动调度，业务访问将会中断。

- 如果业务配置的高防实例，包含多条相同高防线路，且优先级相同时，则按负载均衡方式进行调度，将访问流量平均分发至这些相同运营商的高防线路上进行处理。

示例

假设您拥有高防实例：BGP 高防 IP 1.1.1.1和1.1.1.2、电信高防 IP 2.2.2.2、联通高防 IP 3.3.3.3，其中1.1.1.1、2.2.2.2和3.3.3.3的优先级都为1，1.1.1.2的优先级为2。正常情况下，所有流量被调度至当前优先级为1的一组高防线路进行分发处理，因此来自联通的流量调度到3.3.3.3进行处理，来自电信的流量调度到 2.2.2.2进行处理，来自其他运营商的流量调度到1.1.1.1进行处理。当1.1.1.1进入封堵时，该 IP 下的访问流量将自动调度到2.2.2.2进行处理，当1.1.1.1和3.3.3.3都被封堵时，则原本调度至1.1.1.1和3.3.3.3的访问流量，都将分发至2.2.2.2进行处理，当该组高防线路全部进入封堵时，流量将被调度至1.1.1.2进行处理。

前提条件

- 在开启智能调度前，请将需要防护的业务接入高防实例进行防护。

  说明：

  - 若您需要将防护的云上产品 IP 添加至已购买的高防包实例，请参见 DDoS 高防包 快速入门 。
  - 若您需要将四层或七层业务添加至已购买的 DDoS 高防 IP 实例，请参见 DDoS 高防 IP 接入非网站业务 或 接入网站业务 。
  - 若您需要将防护业务添加至已购买的 DDoS 高防 IP 专业版实例，请参见 DDoS 高防 IP 专业版 业务接入 。

- 在修改 DNS 解析前，您需要成功购买域名解析产品，例如腾讯云的 DNS 解析 DNSPod。

设置线路优先级

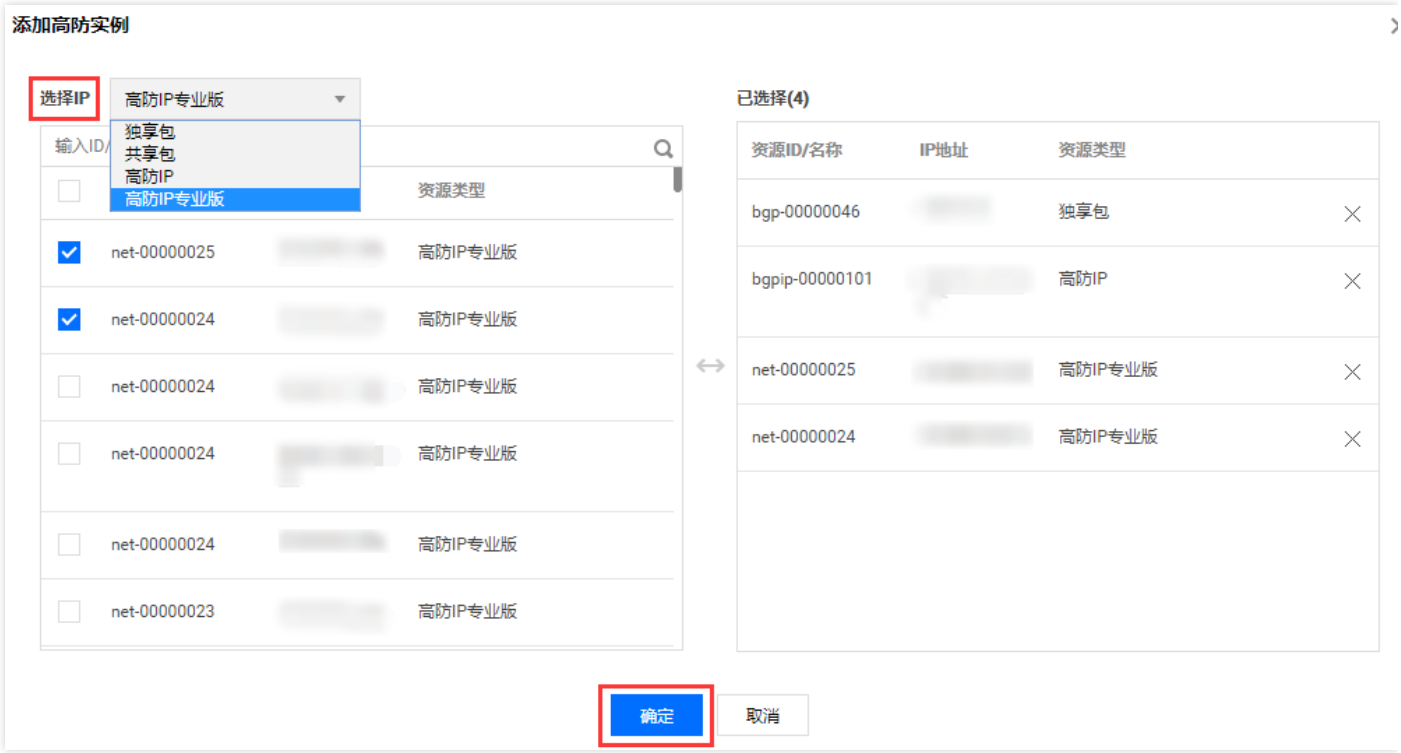
请参考以下步骤，按照设想的调度方案为您的高防线路设置优先级：

1. 登录 DDoS 防护管理控制台，在左侧导航栏选择【智能调度】>【域名列表】，进入域名列表页面，单击【创建智能调度】，系统自动生成一个 CNAME 记录。

2. 找到该 CNAME 记录所在行，单击【添加高防实例】，进入智能调度编辑页面。

3. 在智能调度编辑页面中，TTL 值默认60秒，取值范围为1 - 3600（秒），调度方式为默认优先级。

4. 进入添加高防实例页面，勾选需要设置高防线路优先级的实例，可选高防实例包括独享包、共享包、DDoS 高防 IP 和 DDoS 高防 IP 专业版，单击【确定】。



5. 选择高防实例后，实例的高防线路默认开启域名解析，再为其设置优先级。

示例

例如，您想要将业务流量先调度到 BGP 高防线路，当 BGP 高防线路被攻击遭到封堵后，将流量自动调度到电信高防线路。如果电信高防线路也被封堵，则将流量调度到联通高防线路。当 BGP 高防线路的封堵解除后，流量将自动恢复调度至 BGP 高防线路。
优先级设置方式：您可以将防护业务的高防实例中属于 BGP 高防线路的优先级设置成1、电信高防线路的优先级设置成2、联通高防 IP 线路的优先级不变，即可满足上述调度方案。

如果您暂时不希望联通高防 IP 线路加入流量调度机制，单击  关闭域名解析即可，后面再根据需要重新开启域名解析并设置优先级。若想从当前调度机制中剔除该线路，可直接找到该线路对应实例所在行，单击【解除绑定】即可。

修改 DNS 解析

使用 CNAME 智能调度前，建议您将业务域名 DNS 的 CNAME 记录，修改为 DDoS 防护智能调度系统自动生成的 CNAME，使所有用户访问业务网站的流量都牵引至高防系统。

1. 登录腾讯云 DNS 解析 DNSPod 控制台，在左侧导航栏中，单击【域名解析列表】，在域名解析列表页面，找到目标域名所在行，单击【解析】。

2. 选择【记录管理】>【添加记录】，记录类型选择 CNAME，记录值内输入智能调度系统自动生成的 CNAME 地址，单击【保存】。


全部项目
记录管理
负载均衡
解析量统计
域名设置
自定义线路
线路分组
注意：在中国大陆地区开展网站服务，请先将域名进行备案，否则将无法正常访问。开始备案
请到域名注册商处将DNS修改为：ns3.dnsv5.com ns4.dnsv5.com
修改DNS服务器需要最长72个小时的全球生效时间，请耐心等待。
遇到问题？查看FAQ文档
添加记录
快速添加网站/邮箱解析
暂停
开启
删除
分配至项目
主机记录
记录类型
线路类型
记录值
MX优先级
TTL（秒）
最后操作时间
操作
CNAME
默认
600
保存
取消

配置攻击告警阈值

最近更新时间：2019-12-23 15:29:12

应用场景

当您所使用的 DDoS 高防包遭受攻击、受攻击结束、被封堵以及解除封堵时，系统将以站内信、短信、邮件或微信的方式向您推送攻击告警信息。为更加合理、准确地推送攻击告警信息，减少困扰，新增攻击告警阈值配置功能。若检测的指标超过您设定的阈值，将触发告警，并向您推送攻击告警信息。若发生正常业务操作（如同步数据等）引起流量突增，但被判定为攻击的现象，该功能可以较好地过滤这类情况，帮助您更加准确、清晰地掌握当前业务遭受的攻击状况。如何接收告警信息，请参见 设置安全事件通知。

配置 DDoS 攻击告警阈值

本配置示例可实现如下功能：当高防系统检测到独享型高防包实例“bgp-000005w1”的入流量带宽超过1000Mbps时，将向指定用户群体发送 DDoS 攻击告警信息。

> 注意：
> 需要开启 DDoS 防护状态，才可设置攻击告警阈值。

1. 登录 DDoS 防护控制台，在左侧导航栏中，选择【DDoS 高防包】>【资产列表】，进入 BGP 高防包页面，单击【独享包】，找到高防包实例“bgp-000005w1”，单击实例所在行的操作项【防护配置】。

2. 进入 DDoS 防护配置页面，在 DDoS 攻击告警阈值右侧的下拉框，选择告警指标【入流量带宽】，并设置阈值为1000Mbps。

注意：
DDoS 攻击告警阈值默认【未设置】，支持可选的告警指标有【入流量带宽】和【清洗流量】。

配置 CC 攻击告警阈值

本配置示例可实现如下功能：独享型高防包实例"bgp-000006i9"触发 CC 防护后，当 CC 防护峰值超过2000QPS 时，将向指定用户群体发送 CC 攻击告警信息。

注意：
需要开启 CC 防护状态，才可设置攻击告警阈值。

1. 登录 DDoS 防护控制台，在左侧导航栏中，选择【DDoS 高防包】>【防护配置】，进入防护配置页面，选择【独享包】>【CC 防护】。

2. 开启【CC 防护】，在 CC 攻击告警阈值处，设置阈值为2000QPS。

查看统计报表

最近更新时间：2020-02-12 10:38:38

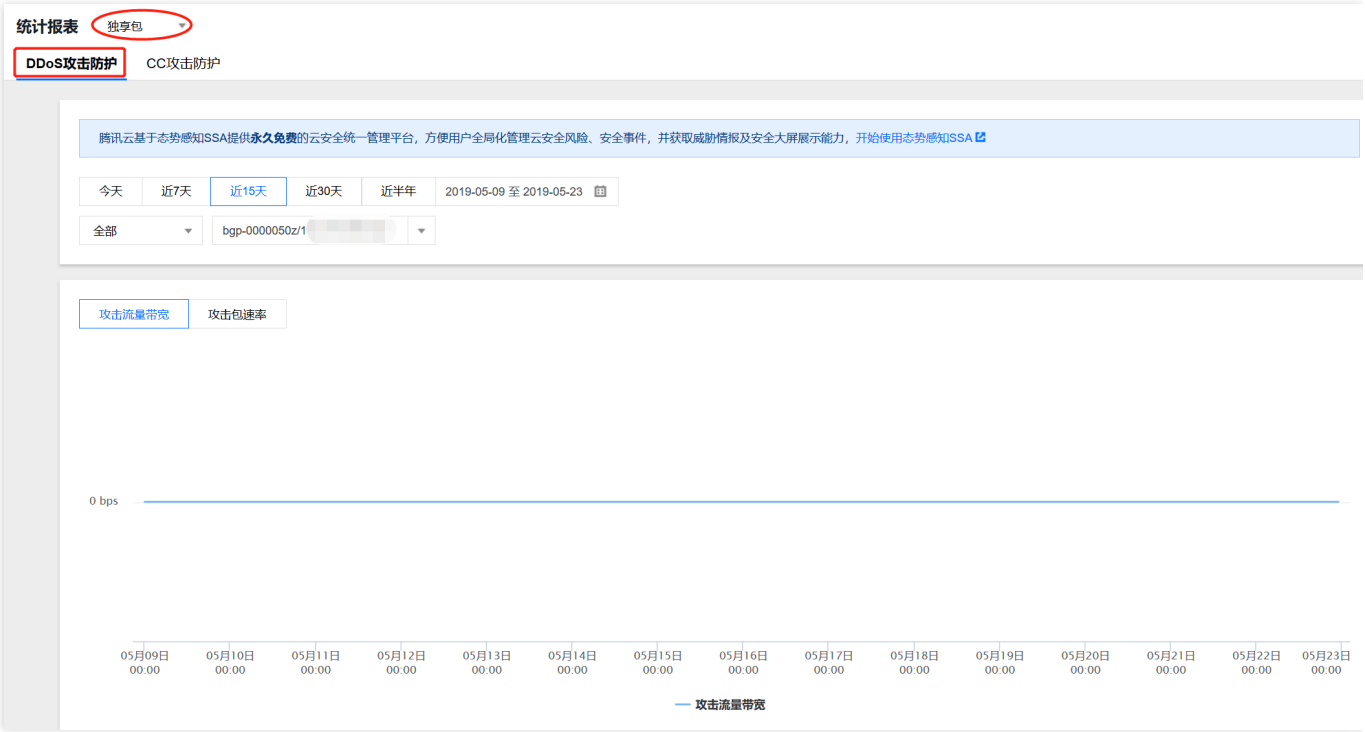
将防护 IP 接入到 DDoS 高防包服务后，当用户收到 DDoS 攻击提醒信息或发现业务出现异常时，需要快速了解攻击情况，包括攻击流量大小、防护效果等，可在控制台进行查看。在掌握足够信息后，才可以采取更有效的处理方式，第一时间保障业务正常。

查看 DDoS 攻击防护情况

1. 登录 DDoS 防护管理控制台。
2. 定位到【DDoS 高防包】>【统计报表】。选择【独享包】。
   说明：当选择【共享包】，可查看该类型高防包中每个防护 IP 的 DDoS 攻击防护情况。
3. 在【DDoS 攻击防护】页签，设置查询时间范围，选择目的地域和高防包实例，查看是否存在攻击。

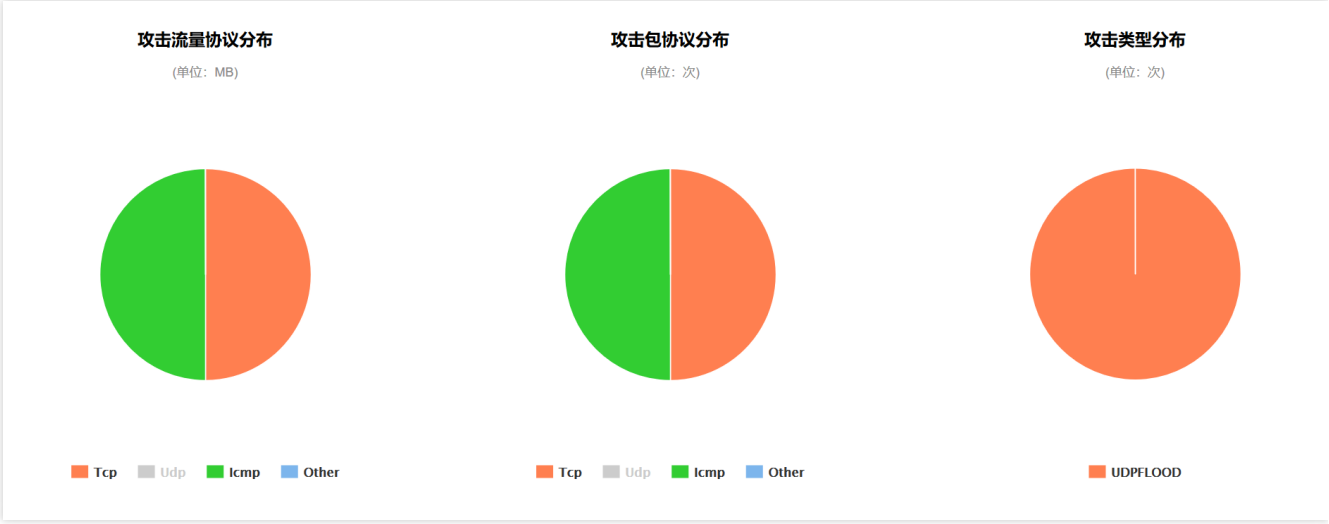
> 说明：
> 支持查询最多180天以内的攻击流量信息及 DDoS 攻击事件。

- 查看该时间范围内所选择的高防包防护遭受的攻击情况，包括网络**攻击流量带宽 / 攻击包速率**趋势。

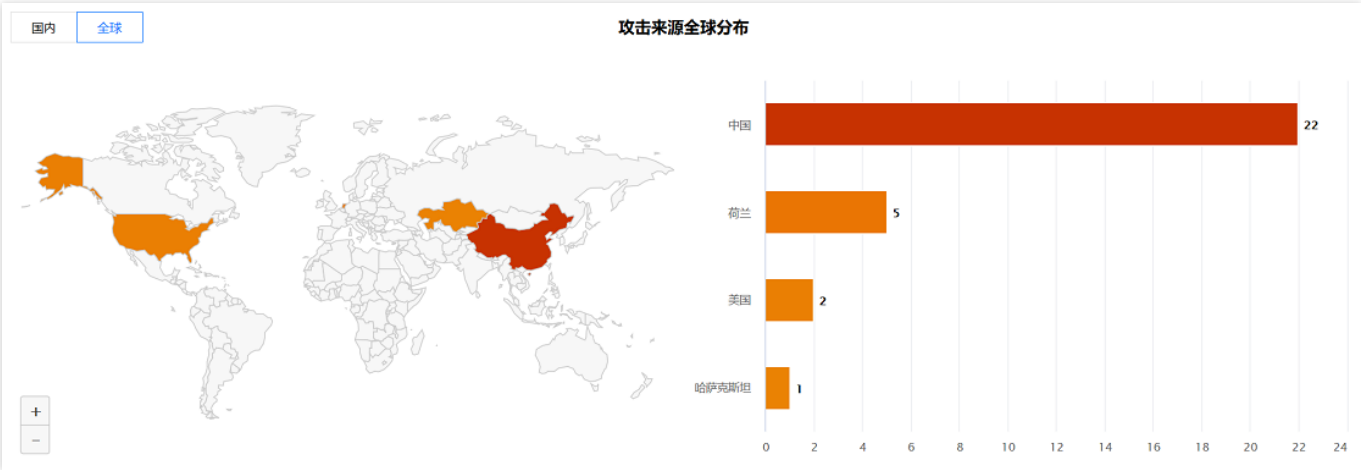


- 通过攻击流量协议分布、攻击包协议分布和攻击类型分布，查看这三个数据维度下的攻击分布情况。

- **攻击流量协议分布**：查看该时间范围内，所选择的高防包实例遭受攻击事件中各协议总攻击流量的占比情况。
- **攻击包协议分布**：查看该时间范围内，所选择的高防包实例遭受攻击事件中各协议攻击包总数的占比情况。
- **攻击类型分布**：查看该时间范围内，所选择的高防包实例遭受的各攻击类型总次数占比情况。



- 在“攻击来源分布”区域查看该时间范围内，所遭受 DDoS 攻击事件的攻击源在国内、全球的分布情况，便于用户清晰了解攻击来源情况，为进一步防护措施提供基础依据。



- 在“DDoS 攻击记录”区域查看该时间范围内，所遭受的 DDoS 攻击事件，了解每一次攻击事件的攻击（开始）时间、持续时间、攻击类型以及攻击状态。
  - 支持攻击包下载，供用户进行 DDoS 攻击分析及溯源支撑。
  - 单击【攻击详情】，了解 DDoS 攻击事件中的最大包速率、最大攻击流量带宽和总的清洗流量情况。
  - 单击【攻击源信息】，查看该时间范围内，所遭受攻击的攻击源 IP 地址、来源地区、产生的攻击流量及攻击包量大小等信息。

> 注意：

攻击源信息为抽样数据，即随机抓包统计的数据，在攻击结束后大约2小时才会显示数据。

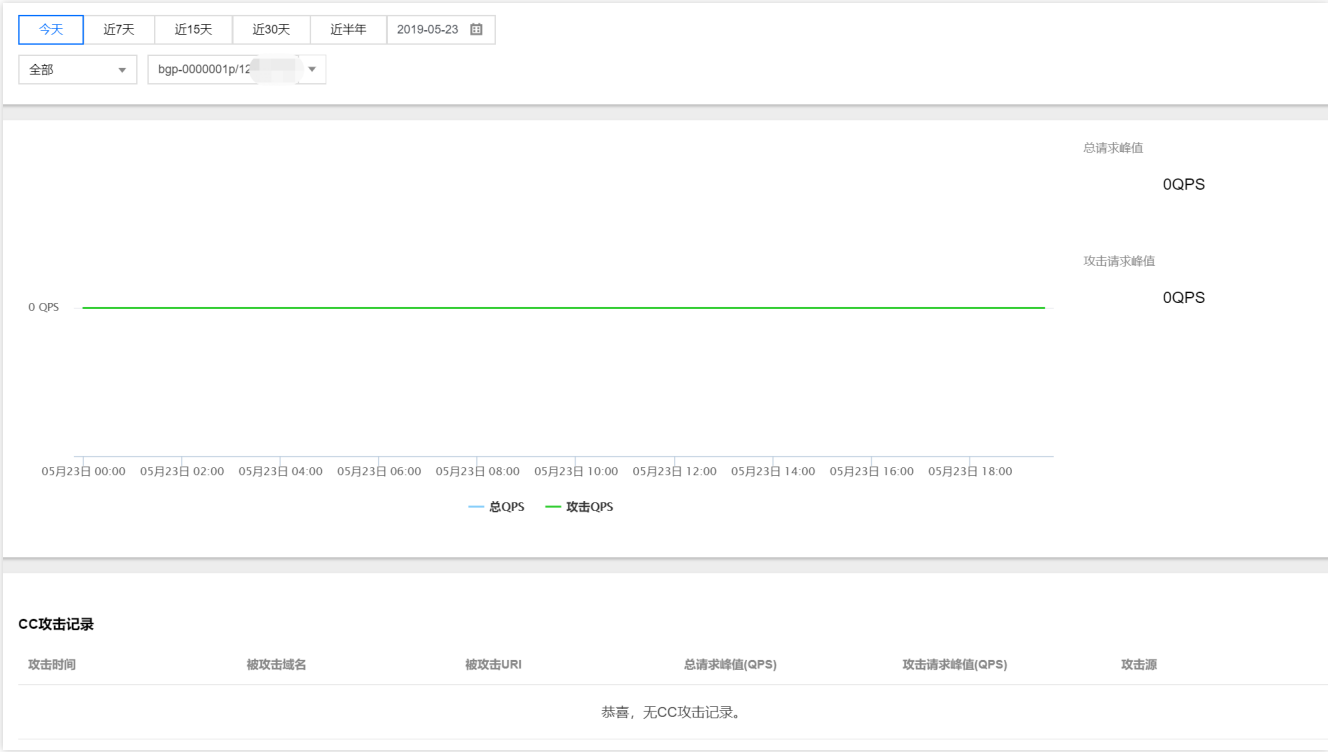
查看 CC 攻击防护情况

1. 登录 DDoS 防护管理控制台。
2. 定位到【DDoS 高防包】>【统计报表】，选择【独享包】。
   说明：当选择【共享包】，可查看该类型高防包中每个防护 IP 的 CC 攻击防护情况。
3. 单击【CC 攻击防护】页签，设置查询时间范围，选择目的地域和高防包实例，查看是否存在 CC 攻击。

说明：
支持查询最多180天以内的攻击请求数信息及 CC 攻击事件。

- 用户可以选择【今天】查看所选择的高防包的攻击请求数趋势。通过观察总请求值是否远高于正常情况下的业务访问量（QPS），并查看攻击 QPS 是否有数值且数值超大。
- 如果存在 CC 攻击，系统会记录下攻击的开始时间、结束时间、被攻击域名、被攻击 url、总请求峰值、攻击请求峰值和攻击源等信息。
  - **总请求峰值**：统计遭受攻击时，高防包接收到的总请求流量峰值。

- **攻击请求峰值**：统计遭受攻击时， 由高防系统阻断的请求次数峰值。



查看操作日志

最近更新时间：2019-12-23 15:29:21

操作场景

DDoS 高防包支持查看近90天内重要操作的日志，如有需要，您可以登录 DDoS 防护管理控制台 查看。可查看的日志包含以下类别：

- 防护对象 IP 更换日志
- DDoS 高级防护策略变更操作日志
- 清洗阈值调整日志
- 防护等级变更日志
- CC 防护策略变更操作日志
- 弹性防护峰值调整日志
- 资源名称的修改日志

操作步骤

1. 登录 DDoS 防护管理控制台。

2. 选择【操作日志】，进入操作日志查询页面。

3. 设置时间范围，通过【产品类型】筛选【独享包】或【共享包】，查看对应的操作记录。

> 说明：
>
> - 独享包：指提供单个 IP 独享 DDoS 防护能力的 DDoS 高防包。
> - 共享包：指提供多个 IP 共享 DDoS 防护能力的 DDoS 高防包。

版权所有：腾讯云计算（北京）有限责任公司

设置安全事件通知

最近更新时间：2020-04-01 16:48:51

操作场景

当您所使用的高防包防护 IP 受到攻击、受攻击结束、IP 被封堵以及解除封堵时，将以站内信、短信、邮件、微信或者电话的方式，向您推送告警信息：

- 攻击开始时，您将会收到攻击开始提示。
- 攻击结束后15分钟，您将收到攻击结束提示。
- IP 被封堵时，您将收到封堵提示。
- IP 解除封堵时，您将收到解除封堵提示。

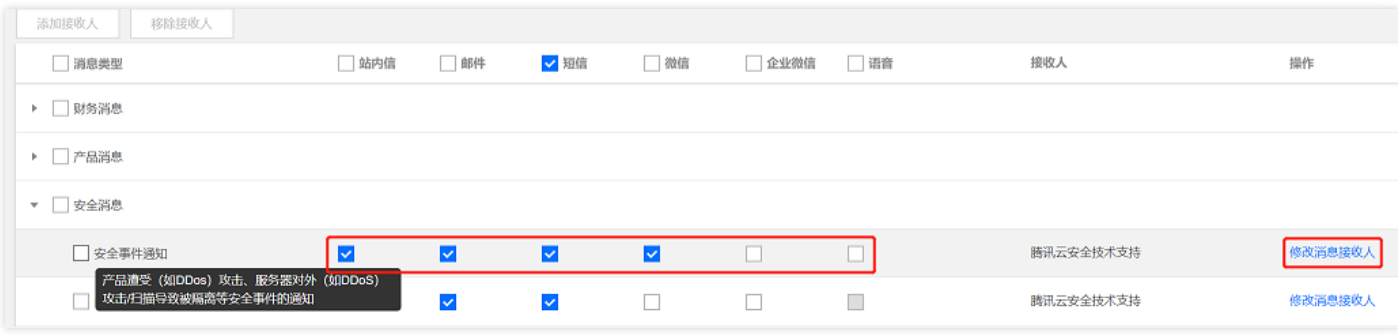
您可以根据实际情况修改告警信息的接收人和接收方式。

操作步骤

1. 登录您的腾讯云账号，进入 消息中心。

> 说明：
>
> 您也可以登录 控制台，单击右上角的 ，在弹出页面单击【查看更多】，进入消息中心。

2. 在左侧目录中单击【消息订阅】，进入消息列表。
3. 在消息列表中，在安全事件通知所在列，选择接收方式，单击【修改消息接收人】，进入修改消息接收人页面。



4. 在修改消息接收人页面，进行消息接收人的设置，设置完成后单击【确定】即可。