DDoS 基础防护

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】

©2013-2023 腾讯云版权所有

本文档（含所有文字、数据、图片等内容）完整的著作权归腾讯云计算（北京）有限责任公司单独所有，未经腾讯云事先明确书面许可，任何主体不得以任何形式复制、修改、使用、抄袭、传播本文档全部或部分内容。前述行为构成对腾讯云著作权的侵犯，腾讯云将依法采取措施追究法律责任。

【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。未经腾讯云及有关权利人书面许可，任何主体不得以任何方式对前述商标进行使用、复制、修改、传播、抄录等行为，否则将构成对腾讯云及有关权利人商标权的侵犯，腾讯云将依法采取措施追究法律责任。

【服务声明】

本文档意在向您介绍腾讯云全部或部分产品、服务的当时的相关概况，部分产品、服务的内容可能不时有所调整。
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默示的承诺或保证。

【联系我们】

我们致力于为您提供个性化的售前购买咨询服务，及相应的技术售后服务，任何问题请联系 4009100100。

文档目录

操作指南

操作总览

最近更新时间：2022-07-25 17:53:03

您在使用 DDoS 基础防护时，可能碰到查看 DDoS 基础防护信息、统计报表、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 基础防护的常用操作。

DDoS 基础防护

- 查看防护配置
- 设置 DDoS 攻击告警阈值
- 解封防护 IP

统计报表

查看统计报表

安全事件通知

设置安全事件通知

防护概览

最近更新时间：2023-03-20 14:53:52

部署在腾讯云的业务会免费附赠基础防护，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。

查看攻击概览

登录 DDoS 防护（新版）控制台，在左侧导航栏中，单击**防护概览** > **DDoS 基础防护**，在 DDoS 基础防护页面的攻击概览模块中，可查看总防护次数、 基础防护云资产和受到攻击的云资产。

字段说明：

- 总防护次数：近一年内受基础防护的所有云资产被防护的总次数。
- 基础防护云资产：云内受基础防护的所有资产，不包含接入高级防护资产。
- 受到攻击的云资产：近一年内受基础防护的所有云资产，被攻击的资产个数。

查看 DDoS 攻击防护情况

1. 在 DDoS 攻击防护页签，设置查询时间范围，选择目的地域、设备类型和资源 IP，查看是否存在攻击。默认展示全量资产的 DDoS 攻击数据。

> **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。

2. 查看该时间范围内所选择的资源遭受的攻击情况，包括网络攻击流量带宽 / 攻击包速率趋势。

> **说明**
> 此处数据为该时间段全量实时数据。

3. 在近期安全事件模块中，可展示所遭受的 DDoS 攻击事件。
   - 选择所需事件，单击**查看详情**，右侧将展示该事件的具体详情。支持查看攻击源信息、攻击源地区、产生的攻击流量及攻击包量大小等。供用户进行 DDoS 攻击分析及溯源支撑。

   - 选择所需事件，单击**攻击包下载**，在攻击包列表中，选择所需 id，可下载本次攻击计时间段的攻击包采样数据，详细了解攻击数据和类型，用户制定针对

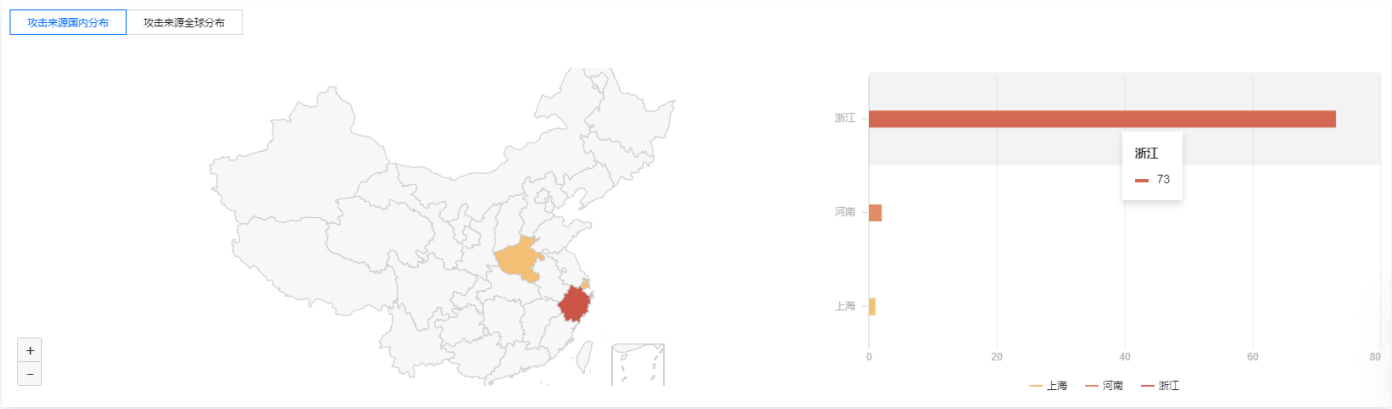
性的防护方案提供数据支撑。

4. 在攻击统计模块中，可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。

字段说明：

- 攻击流量协议分布：查看该时间范围内，所选择的资源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，所选择的资源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，所选择的资源遭受的各攻击类型总次数占比情况。

5. 在攻击来源模块中，可查看该时间范围内，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。



使用限制

最近更新时间：2021-09-10 17:43:42

防护对象限制：为腾讯云内 CVM、CLB 及 NAT 网关等云产品，提供免费的基础 DDoS 防护。

版权所有：腾讯云计算（北京）有限责任公司

查看防护配置

最近更新时间：2023-02-13 16:31:22

操作场景

登录 DDoS 防护管理控制台，可查看 DDoS 基础防护的防护详情，修改防护配置。

操作步骤

1. 登录 DDoS 防护管理控制台，单击 **DDoS 基础防护**，选择服务器类型和地区。

2. 在基础防护页面，单击“目标主机名称”。

3. 在 DDoS 攻击防护页面，支持查看 DDoS 攻击事件详情。

> **说明**
> - DDoS 防护默认为开启状态，当攻击发生时，将触发 DDoS 流量清洗防护，高防系统会对流量进行识别，并过滤恶意流量。
> - 黑洞触发阈值：显示当前该资源的防护阈值；表示当攻击流量超过阈值，将会触发封堵，导致一段时间内业务不能正常访问。如需提高 DDoS 防护能力，可根据业务需要，购买 合适规格的高防产品 。

设置 DDoS 攻击告警阈值

最近更新时间：2022-10-24 11:00:36

操作场景

在 DDoS 防护管理控制台，可查看 DDoS 基础防护的防护详情，并可以对防护 DDos 攻击设置告警阈值。

操作步骤

1. 登录 DDoS 防护管理控制台，在左侧导航中，单击 **DDoS 基础防护**。
2. 单击**设置 DDoS 攻击告警阈值**，弹出设置告警阈值弹窗。

3. 在设置告警阈值弹窗中，DDoS 攻击告警阈值可以选择默认、入流量带宽或清洗流量功能，并设置告警阈值，单击**确定**，即可保存设置。

首次进入，告警策略类型为“默认”。参数说明如下：

- 默认：当攻击流量满足以下其中一条，即发起告警。
  - DDoS 攻击：当攻击入流量 >= 2Gbps或者清洗流量 > 100Mbps。任一条件满足，即发起告警。
  - CC 攻击：当攻击入流量 > 1000QPS。
- 入流量带宽：检测出的攻击流量带宽。当入流量 >= 设置数值即发起告警。
- 清洗流量：被清洗的攻击流量。当清洗流量 >= 设置数值即发起告警。

版权所有：腾讯云计算（北京）有限责任公司

解封防护 IP

最近更新时间：2023-05-12 16:53:22

当用户公网 IP 被大流量 DDoS 攻击，且攻击流量超过了 DDoS 基础防护能力时。为了避免攻击对用户业务造成更大影响，以及避免对腾讯云内其他用户造成影响，对用户 IP 进行封堵，避免更大的损失。默认情况下封堵时长为2-24小时。封堵结束后，将自动解封。

解封被封堵 IP

DDoS 高防包和 DDoS 高防 IP 用户拥有自助解封次数，DDoS 基础防护的用户无自助解封次数。 建议购买高防产品：DDoS 高防包 和 DDoS 高防 IP，避免业务因为封堵而受到影响。

> **说明**
> 封堵状态中的 IP 接入高防产品也可解除封堵。

设置安全事件通知

最近更新时间：2022-11-30 17:36:22

操作场景

当您所使用的腾讯云公网 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。

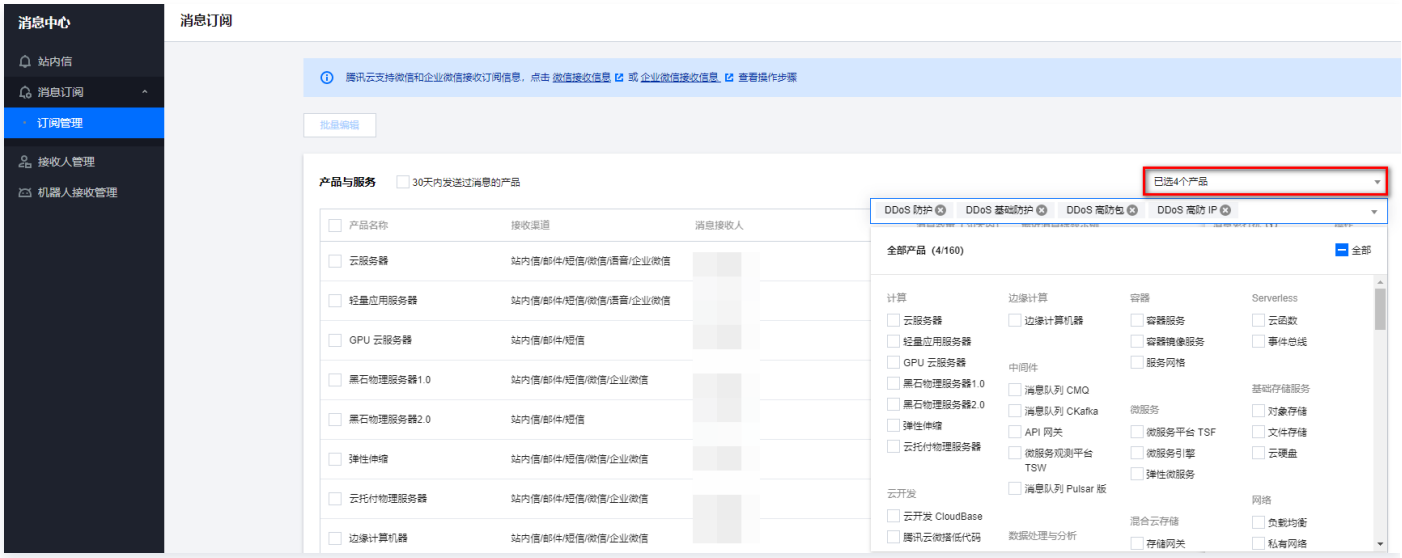
您可以根据实际情况修改告警信息的接收人和接收方式。

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 > 订阅管理**，并选择需要接收消息的产品。



3. 在消息订阅页面，选择接收方式，单击**编辑**。

4. 在订阅编辑弹窗中，进行消息接收人的设置，设置完成后单击**确定**即可。


订阅编辑
邮箱、手机、微信未验证的用户将无法接收邮件、短信、语音、微信消息，验证通过并开启对应接收方式后即可接收
非企业微信子用户无法接收企业微信消息，企业微信子用户且在腾讯云助手应用的成员可见范围内方可接收企业微信消息。
产品名称
DDoS 基础防护
接收模式
免打扰
开启后，该产品的短信、语音、微信消息将无法接收，站内信、邮件、企业微信消息正常接收（勾选该类消息通道时），
免打扰模式下，无法编辑消息接收人及消息通道
接收渠道
站内信
邮件
短信
微信
语音
企业微信
消息接收人
用户
用户组
IM应用
机器人
新增消息接收人
修改接收人联系方式
已选择(1)
搜索用户名称
用户名称
用户类型
手机号码
邮箱
微信
主账号
已验证
接收人名称
接收人类型
主账号
定制化配置产品子消息 点击进入高级编辑模式
确定
取消