

目录

目录	1
调整防护能力	2
操作步骤	2
重要说明	2
调整带宽	2
操作步骤	2
重要说明	2
分配至项目	2
加入项目制	2
更改防护实例项目制	3
防护配置	3
前提条件	3
规则模板说明	3
配置防护模板	3
地域封禁	3
统计数据	4
基础数据展示	4
IP受攻击统计（30天）	4
DDoS攻击记录	4

调整防护能力

本文档介绍了为高防弹性IP实例进行防护能力调整的操作流程。

操作步骤

1. 登录[高防弹性IP控制台](#)。
2. 选择防护实例，单击**调整防护能力**按钮。



3. 在**调整防护实例**的对话框中调整防护能力和弹性上限。
4. 单击**立即支付**按钮后，跳转到确认订单页面。
5. 核对订单配置后，单击**提交订单**。
6. 产品服务状态更新为**已开通**，则表示调整成功。

重要说明

弹性上限为防护实例最高防护能力，可调整的值与您所购买开通的防护能力套餐有关，每个保底防护能力能够支持的最大弹性上限详见[价格总览](#)。

调整带宽

本文档介绍了为高防弹性IP防护实例进行带宽调整的操作流程。

操作步骤

1. 登录[高防弹性IP控制台](#)。
2. 选择防护实例，单击**调整带宽**。
3. 在调整带宽对话框中调整带宽值。



4. 单击**立即支付**按钮后，跳转到确认订单页面。
5. 核对订单配置后，单击**提交订单**。
6. 产品服务状态更新为**已开通**，则表示带宽调整成功。



重要说明

- 带宽值为防护实例下所有IP共享带宽。
- 增强型95付费按实际月95峰值带宽计费，保底带宽等于实例的带宽值乘以保底比例。

分配至项目

高防弹性IP支持项目制，其中IP的项目制与防护实例的项目制一致。

加入项目制

您可以在新购高防弹性IP防护实例时，选择**所属项目**，防护实例与IP将加入到相同的项目制中。



更改防护实例项目制

您可在高弹性IP控制台进行防护实例的项目制变更。

1. 登录[高弹性IP控制台](#)，选择防护实例，点击**分配至项目**。



2. 选择要分配的项目制，点击**确定**，分配至项目成功。
3. 返回防护实例列表，确认项目变更成功。



防护配置

本文档介绍了高弹性IP防护规则的相关说明及配置防护规则的操作流程。

前提条件

1. 您已成功[购买高弹性IP\(高防包\)](#)实例。
2. 本文档介绍的防护配置仅作用于2021年6月2日以后创建的防护实例，若您需要调整旧实例的防护配置，请及时联系售后人员。

规则模板说明

规则模板作用于防护实例，实例内所有IP均按模板规则进行防护。

默认	宽松	严格
全局TCP连接数不限制	全局TCP连接数不限制	全局TCP连接数不限制
并发连接数不限制	并发连接数不限制	并发连接数不限制
全局TCP流入带宽不限制	全局TCP流入带宽不限制	全局TCP流入带宽不限制
单用户SYN发送频率限制1秒200个包	单用户SYN发送频率限制1秒500个包	单用户SYN发送频率限制1秒100个包
单用户TCP最大连接数10000	单用户TCP最大连接数20000	单用户TCP最大连接数5000
单用户TCP每秒新建连接数500	单用户TCP每秒新建连接数1000	单用户TCP每秒新建连接数250
UDP带宽限制10G	UDP带宽限制15G	UDP带宽限制5G

配置防护模板

登录[高弹性IP防护页控制台](#)，选择要配置的实例，所有实例默认应用**系统策略-默认**模板进行防护，UDP封禁功能默认为开启状态。



地域封禁

通过设置地域封禁，针对指定的中国内地省份或国际港澳台地区的来源IP进行一键封禁。功能默认关闭，目前仅支持封禁海外IP。



统计数据

数据统计功能将于近期开放到控制台，敬请期待

基础数据展示

基础数据展示支持按IP粒度或防护实例粒度，展示连接详情和实时带宽数据。

IP受攻击统计（30天）

按照IP粒度展示30天内被攻击IP的受攻击记录，包括被攻击次数、攻击峰值、攻击总流量。

IP受攻击统计（30天）

IP实例	被攻击次数	攻击峰值	攻击总流量
------	-------	------	-------

DDoS攻击记录

展示被攻击IP的详细DDoS攻击记录，包括开始时间、结束时间、攻击类型、攻击峰值、峰值PPS、持续时间、攻击状态。

DDoS攻击记录

IP	开始时间	结束时间	攻击类型	攻击峰值	峰值PPS	持续时间
----	------	------	------	------	-------	------