

# 云防火墙 故障处理





【版权声明】

©2013-2024 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或95716。



# 文档目录

故障处理 云防火墙误报误拦截应急预案



# 故障处理

# 云防火墙误报误拦截应急预案

最近更新时间: 2024-04-24 17:51:21

本文档将为您介绍,当入侵防御误报,导致大量异常拦截,或因策略变更有误,导致流量出现异常下跌情况时,需要如何处理。

## 现象描述

IP 地址出现入侵防御误报导致的大量异常拦截,或因策略变更有误,导致流量出现异常下跌。

#### 解决思路

当确认拦截的来源是云防火墙后,可以先止损(如关闭拦截功能)、再排查、最后交由产品安全团队人工处理。

### 处理步骤

## 步骤1:关闭拦截功能

- 1. 登录 云防火墙控制台,在左侧导航中,单击入侵防御。
- 2. 在入侵防御页面,将防护模式切换为**观察模式**。

防护模式	◯ 观察模式	◯ 拦截模式	○ 严格模式 ?	剔除资产

3. 在拦截列表上方,关闭"启用拦截列表"的功能开关。

拦截列	<b> 表</b> 忽略列表										
添加	地址 删除地址	全部方向	* 技	起始生效时间倒序	▼	目拦截列表	多个关键字用竖线 " " 分隔,	多个过滤标签用回车键分隔		Q,	φ
	恶意IP地址	危险等级 🔻	地理位置	拦截方向	安全事件来源 🔻	生效时间		拦截次数		操作	
		中危	AU1010-	入站	基础防御(严格模式)	2021-04-08 15:26:05 至	2021-04-09 15:26:05	0	编辑	删除	
	1000	低危	ABUTURG -	入站	威胁情报(严格模式)	2021-04-08 15:24:13 至	2021-04-09 15:24:13	0	编辑	删除	

## 步骤2:手动处置

- 1. 登录 云防火墙控制台,在左侧导航栏中,单击告警中心,进入告警中心页面。
- 2. 在告警中心页面,选择**阻断拦截统计 > 入站方向**。
- 3. 在入站方向页签,选择按拦截统计排序,找到误拦截的 IP。

入站方向	出站方向												
一键放通	全部状态	Ŧ	按拦截统计排序	•	拦截频率统计:分钟	Ŧ		多个关键字用竖线 "[" 分隔,	多个过滤标签用回	车键分隔	Q	¢:	] 资产视角
访问源 地理位置	1 中国浙江省杭州	M (	按最近拦截时间排序 按拦截统计排序 按平均拦截频率排序 资产名称	<b></b>	(3) (4)		实时拦截 最后一次 平均拦截	线统计 138 2021-04-07 11:44:52 频率 0.23/分钟	判断来源	入侵防御:	基础防御	D	置顶 放通 封禁

- 4. 将误拦截 IP 加入白名单。
  - 方式1:在误拦截 IP 右侧,单击放通,可将 IP 地址加入到白名单(忽略列表),放行该 IP 的后续访问。
  - 方式2:在 入侵防御 页面,选择忽略列表 > 添加地址,将误报的 IP 地址批量加入到白名单。



	拦截列	し しょうしょう しょう	忽略列表										
	添加	地址	删除地址	全部方向	•	按起始生效时间倒序	v		多个关键字用竖线 " " 分隔,	多个过滤标签用回车键分隔		Q,	φ
Ī		恶意1	危险等级 ▼	地理	忽略方向	安全事件来源 🍸	忽略原因 ▼	生效时间		忽略次数		操作	
		-	未知	+8	入站	手动添加	-	2021-04-07 21:22:35 至 永久	۲.	53	编辑	删除	
		181.	未知	÷2.	入站	手动添加	-	2021-04-07 21:22:35 至 永公	z	40	编辑	删除	

5. 处理完成后,恢复 步骤1 的配置,观察流量是否正常。

## 步骤3:提交工单反馈误报

1. 若手动处置完毕,仍存在流量异常,可进入 提交工单 页面,提供 AppID 与误报的 IP 地址给安全团队确认。

2. 安全团队收到反馈后,会在规定时间内快速响应,调整检测规则。