

## DDoS 高防（中国内地）使用指南

### 目录

1. 产品概述
  2. 接入与配置
  3. 防护管理
  4. 日志与监控
  5. 常见问题解答
  6. 技术支持与服务
- 

### 1. 产品概述

DDoS 高防服务通过超大带宽清洗和智能防护技术，保护企业业务免受 DDoS 攻击，确保业务稳定运行。本服务支持流量型、连接耗尽型和应用层攻击防护，适配电商、游戏、金融等多种场景。

---

### 2. 接入与配置

#### 步骤 1：申请服务

1. 登录管理控制台，选择“DDoS 高防服务”。
2. 根据业务需求选择适合的防护套餐（如带宽和防护类型）。
3. 提交订单并完成支付。

#### 步骤 2：域名或 IP 接入

1. 将业务域名解析到高防 IP（在 DNS 设置中修改 A 记录）。
2. 确保高防 IP 后端配置指向源站服务器。
3. 测试域名访问，确认服务正常运行。

#### 步骤 3：配置防护策略

1. 登录管理后台，进入“防护设置”页面。
  2. 设置防护策略，包括流量阈值、黑白名单、攻击行为拦截等。
  3. 启用防护并保存配置。
- 

### 3. 防护管理

#### 实时监控

- 登录防护控制台查看流量监控数据，包括攻击流量、清洗流量等。
- 配置告警规则，及时接收异常流量通知。

#### 动态调整策略

- 根据业务流量特点，动态调整防护阈值和策略规则，优化防护效果。

#### 攻击日志分析

- 下载攻击日志，分析攻击类型、源 IP 分布和攻击流量趋势，制定更精确的防护方案。
- 

### 4. 日志与监控

#### 日志查看

1. 登录控制台，进入“日志管理”模块。
2. 按时间筛选查看攻击日志，或导出日志文件用于深入分析。

#### 监控报表

- 定期生成流量清洗报表，了解攻击趋势和防护效果。
  - 使用图表可视化工具，直观掌握业务安全动态。
-

## 5. 常见问题解答

Q1: 服务接入后, 业务访问变慢怎么办?

- 检查高防 IP 的后端服务器配置是否正确。
- 确认源站带宽和处理能力是否足够。

Q2: 如何处理误拦截问题?

- 在管理后台调整白名单策略, 允许可信 IP 或域名通过。

Q3: 攻击未完全被拦截, 如何优化?

- 提高防护阈值或升级带宽配置, 确保清洗能力匹配业务流量。
- 

## 6. 技术支持与服务

- 24/7 技术支持: 如有紧急情况, 请通过电话或在线工单联系我们的安全团队。
  - 服务资源中心: 访问帮助文档、视频教程和 FAQ, 获取更多使用指导。
  - 定制化服务: 针对特殊业务需求, 可提供个性化防护方案, 请与客户经理联系。
- 

## 联系我们

如有其他疑问, 请访问我们的官方网站或拨打客服电话。我们将竭诚为您服务