

目录

目录	1
产品概述	2
什么是高防IP	2
技术原理	2
功能概览	2
产品功能	2
产品优势	2
产品优势	2
术语说明	2
DDoS攻击	2
CC攻击	2
DDoS攻击与CC攻击的区别	2

产品概述

什么是高防IP

高防IP (Kingsoft Cloud Advanced Defense, 简称KAD) 为用户已备案的域名提供T级DDoS攻击防护能力。完成高防IP实例配置后, 用户在遭遇大流量DDoS攻击时, 攻击流量被引至高防IP, 确保源站稳定可用。

技术原理

- 金山云高防IP在云端对DDoS攻击进行防御清洗, 通过防护算法拦截攻击流量, 将正常流量转发回源, 高拦截率算法确保攻击能够被有效拦截, 保障业务实时在线。
- 高防IP代理源站IP对外提供服务, 将用户公网流量都引流至高防IP, 源站隐藏在高防IP后端, 攻击者无法直接找到源站, 也就无法对源站发起攻击。高防IP转发原理示意图如下所示:

功能概览

产品功能

- 完整DDoS攻击防御: 可以提供完整的4-7层攻击防御, 包括TCP flood, UDP flood, 反射放大攻击, 应用层CC攻击等常见攻击类型
- 攻击数据查询: 详细的攻击日志和流量图表, 提供透明的攻击状况展示
- 多协议支持: 支持HTTP、HTTPS、TCP, 部分线路支持UDP
- 云外用户接入: 云外用户可无缝接入金山云高防IP
- 提供覆盖电信、联通、移动运营商BGP线路, 单节点防御能力2T。

产品优势

产品优势

- 海量清洗能力: 弹性计费下可防御2000Gbps的DDoS攻击流量
- 高质量网络: 覆盖电信、联通、移动多线BGP运营商接入
- 响应迅速: 高性能设备秒级检测和清洗, 极高的检测准确率
- 高性价比: 可包年包月或包年按次购买, 灵活选择, 多场景支持, 防护成本可控
- 零部署成本: 无需更改网络拓扑, 不需采购设备, DNS切换一键快速接入
- 全业务: 支持TCP, UDP, Http(s)、WebSocket业务协议

术语说明

本文档主要介绍了高防IP的常见术语。

DDoS攻击

全称为分布式拒绝服务攻击(Distributed Denial of Service), 黑客通过控制大量傀儡机, 将其联合起来作为攻击平台, 对一个或多个目标发动DDoS攻击, 从而成倍地提高拒绝服务攻击的威力。

DDoS攻击成本低廉, 攻防极不对等(攻击自动化)。并且攻击造成的影响严重, 攻击目标更有针对性, 比如支付页面、登陆服务、首页等; 游戏行业是遭受DDoS的重灾区。

CC攻击

CC攻击全称Challenge Collapsar, 是DDoS攻击的一种。CC攻击通过代理服务器或者大量肉鸡模拟多个用户访问目标网站的动态页面, 制造大量的后台数据库查询动作, 消耗目标CPU资源, CPU长时间处于100%, 永远都有处理不完的连接直至网络拥塞, 正常的访问被中止。

DDoS攻击与CC攻击的区别

DDoS可以用硬件防火墙来过滤攻击，而CC攻击本身的请求就是正常的请求。CC主要是针对网页的攻击，攻击者控制某些主机，模拟多个用户不停地访问需要大量数据操作的页面，造成服务器资源的浪费。