2023

智安网络

ZHIAN NETWORK

云盾-APP 业务防护系统

技术白皮书

AQ-CP-040 V1.2

市场指南

深圳市智安网络有限公司

www.zhiannet.com

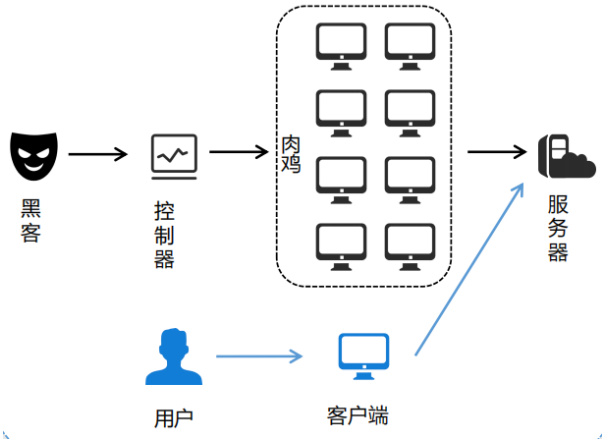
智安网络
ZHIAN NETWORK

目录

1. 背景介绍

1.1. DDoS 攻击现状

自 DDoS 攻击峰值在 2016 年迈入 Tb 级攻击时代后，Tb 级攻击已逾 5 年，超百 G 大流量攻击持续增长，出于敲诈勒索目的的 DDoS 攻击更是层出不穷，俨然成为犯罪团伙首选勒索手段，严重威胁企业安全。



（1） 游戏仍然是攻击热点，出海游戏更易遭受 DDoS 攻击

互联网多元化发展迅速，云计算、视频直播等新兴行业备受用户青睐，DDoS 黑产攻击目标也紧随热点业务产生变化，整体来看，2021 年里游戏仍是受 DDoS 攻击最多的行业。

相比国内发行的游戏，出海游戏更易遭受 DDoS 攻击：一方面，出海企业大多复制国内已验证的成功商业模式，推出的游戏往往颇具竞争力，容易成为海外 DDoS 攻击的目标；另一方面，国外环境比较复杂，以 ACCN 为代表的黑产团队肆无忌惮，出于敲诈勒索目的的 DDoS 攻击层出不穷。

（2） 虚拟货币监管加码，大量肉鸡流入 DDoS 攻击黑产

2021 年下半年以来，国家持续加强整治虚拟货币“挖矿”活动，以改善能源利

用效率， 维护社会稳定和国家安全。大量基于矿机挖矿的企业迁移海外，利用肉鸡进行挖矿的黑产也受到较大冲击。大量肉鸡从虚拟货币挖矿行业流出，进入 DDoS 攻击领域。

黑客手里的肉鸡资源较为富余，在 5 月份之后的几个月，利用肉鸡发起的 UDP flood 攻击大幅高于去年同期水平，甚至 2021 年 7 月一个月的攻击数量都高于 2020 年半年的总和。

（3） 扫段攻击成网络公害，脉冲攻击防不胜防

扫段攻击是近年来兴起的一种攻击方式，和以往攻击者只盯着单个目标 IP 不断变换攻击手法、寻求突破防护策略短板的攻击方式不同，扫段攻击多使用已知的通用攻击手法，攻击期间基本不会变换，但攻击者会在短时间内对大量 IP 进行无差别攻击，令大量攻击流量涌入机房，而防护设备也需要承载大量 IP 上的业务流量，防护系统性能压力大，易造成整个机房业务瘫痪。

除了扫段攻击外，脉冲攻击也成为现网比较典型的攻击手法。黑产团队通过定制攻击工具，以固定时间为间隔，短期内对目标发起高达业务流量千倍大小的攻击流量，随后很短时间内，攻击又消失于无形。这种攻击流量增长快，消失快，攻击密集，不仅让企业的安全运维人员不堪其扰，对防护系统的性能和灵敏度也提出了更高的要求。

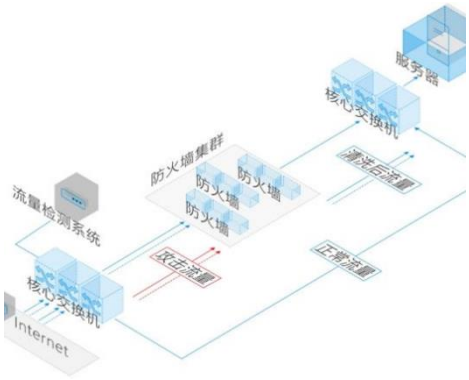
（4） DDoS 威胁或成为犯罪团伙首选勒索手段

勒索软件攻击事件在 2021 年闹得沸沸扬扬，2021 年勒索软件和 DDoS 攻击曾多少同时勒索受害者。犯罪团伙利用勒索软件实施勒索，若受害者不支付赎金，便威胁将数据公之于众。此时，如果受害者报案，犯罪团伙就发起 DDoS 攻击，似图报复。勒索 DDoS 事件前几年已经出现，2020 年和 2021 年勒索团队赚的“盆满钵满”，进一步刺激了 DDoS 攻击团伙的贪欲。而 DDoS 攻击朔源难度较大，勒索实施成本低、收益丰厚，预计未来一段时间内，DDoS 勒索依然对企业安全构成较大威胁。

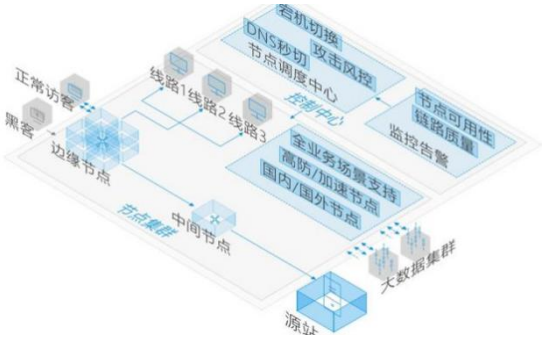
1.2. 传统防御方案

（1） 方案特点

基于高防 IDC 防护方案：以 IDC 为中心，单点服务能力有上限；进攻方有明确目标；防守方通过肉搏的方式对抗，攻击有多大，就储备多大的带宽资源。



基于高防 SaaS 的防护方案：防护前置到边缘节点；通过反向代理方式，隐藏被保护对象，进攻方无法获知攻击目标，实现了替身式云防护；攻击全部牵引到防御节点，依赖于节点池、调度系统、人机识别算法。



（2） 方案劣势

- 防护节点数量有限，攻防资源严重不对等；
- 抗海量攻击能力有限，大攻击情况下，节点稳定性差；
- 节点调度分配集中化，节点宕机切换延迟高，对客户业务影响面大；
- CC 粗颗粒度防护，依赖人工设置防护策略，漏防、误防严重；

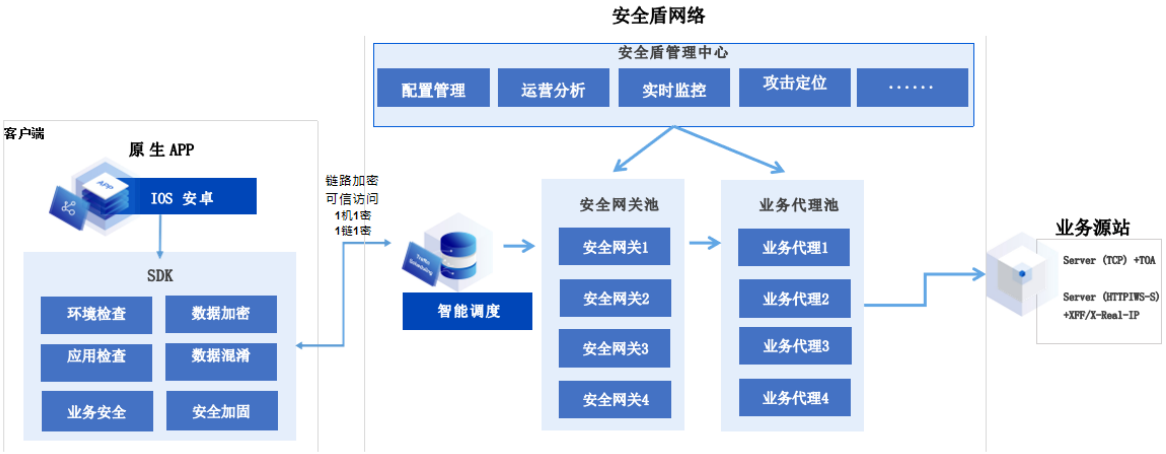
- 防护能力依赖带宽大小和清洗能力，防护成本高；
- DNS 解析生效慢，缓存机制下节点切换延迟高；
- 通过 DNS 解析，节点被暴露，更有 DNS 解析劫持、查询攻击风险；

2. 产品介绍

2.1. 产品简介

智云盾（安全盾），是下一代网络安全技术模块，通过 SDK 嵌入或者 Client 集成方式，用户可自主将安全盾集成到网络应用产品中，提升网络安全性，降低安全防护成本，实现 DNS 防污染、防掉线、应用加速、防 DDoS/CC、故障自愈、源站隐藏、数据分析等安全稳定运营要求。支持 windows、macos、ios、Android 客户端接入，支持 tcp/http/https/websocket/websockets 协议业务。

2.2. 产品架构



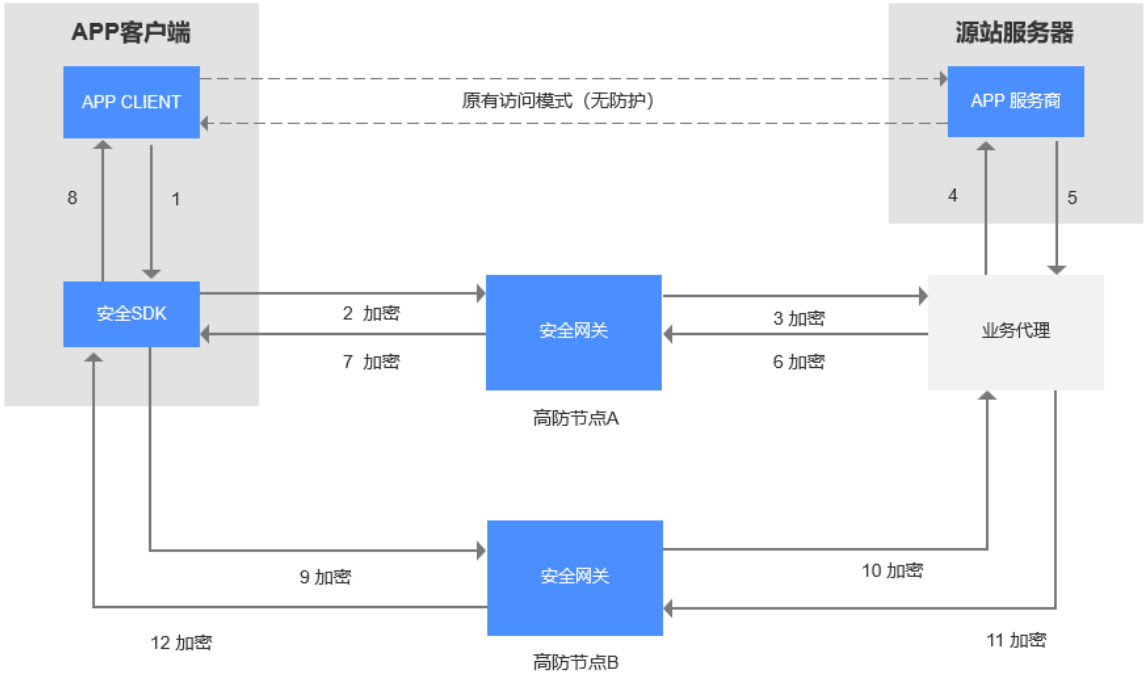
安全盾由三部分组成：客户端、安全盾网络、业务源站，其中客户端包括原始 APP 和安全盾 SDK，安全盾网络包括安全网关池、业务代理池、管理中心，业务源站包括源站程序和真实 ip 获取模块；

客户端侧，需要在原有 APP 代码基础上集成 SDK，打包成新的 APP 端，当 APP 启动时直接访问 127.0.0.1:随机端口，该请求会被 SDK 响应并转发到安全盾网络，通过认证后最终到达业务源站；

安全盾网络侧，安全网关具备高防护能力且分布式部署，不会被攻击穿透，即使被大流量 ddos 攻击打挂，也能快速被 SDK 检测并无缝切换，代理节点发起与业务源站的连接；

业务源站侧，支持 TCP 和 HTTP 类协议业务，安全盾网络能将真实访问 IP 透传到源站，只需要源站安装 TOA 模块或者配置 XFF 或者 X-real-IP。

2.3. 防护原理



- **APP 安全：**APP Client 与 SDK 集成后进行应用加固，通过对 Java/OC/C/C++/Swift 代码进行混淆和 so 代码的保护，防 Java 层调试，防 native 层调试等加固技术可有效防御逆向、恶意注入、数据窃取、二次打包等攻击；
- **传输安全：**SDK 与网关之间通讯使用了特殊加密的消息协议，所以使得攻击者模

拟数据攻击和抓包重放攻击变得困难；

- **网络安全：**由于网关具备高 T 级防护能力，且支持分布式部署和弹性扩容，使得安全盾网络具备较强的 DDoS 防护能力，且由于 SDK 与网关之间采用了特殊加密算法，使得攻击数据无法穿透网关，真正做到零漏防、零误封；
- **DNS 安全：**由于 APP 客户端不涉及 DNS 环节，网关和代理节点也不提供域名服务，完全杜绝了 DNS 和域名带来的种种问题；
- **源站安全：**由于整套系统只对外暴露网关 IP，有效保护了源站 IP 不被暴露，再加上对源站进行 IP 访问限制，可有效拦截网络爬虫和恶意扫描的访问；
- **防掉线功能：**当 2、3、6、7 因为高防节点 A 故障而中断时，SDK 会马上发起新的网关连接（9、10、11、12），并将 1、8、4、5 连接传输的数据通过高防节点 B 传输，无论是客户端还是源站均对高防节点 A 的故障无感知。

2.4. 产品主要功能

- **终端硬件级授权：**精准控制终端设备访问业务系统，轻松实现多因素访问控制要求；
- **先认证再连接的接入流程：**只有集成了 SDK 合法的终端数据才能进入安全盾网络/只有下载了定制浏览器的用户才能进入安全盾网络，精准防御黑客发起的各种网络攻击（DDoS/CC 攻击、入侵攻击、恶意扫描等等）；
- **SDP 网络集群无限扩展：**先进的风控架构体系能够有效隔离风险，网关具备高 T 级防护能力，且支持分布式部署和弹性扩容，使得安全盾网络具备较强的 DDoS 防护能力；
- **终端故障自愈能力：**秒级检测节点，当发生网络波动或节点故障时，自动切换到其他优质节点，且切换过程中安全盾具有无感知续连功能，业务保持不掉线；
- **零暴露面的隐身能力：**服务节点针对终端完全隐身，黑客无法获知攻击目标，无法直接针对服务节点发起全面攻击，接入安全盾前会进行源站泄露检测，如果源站已泄露需要重新更换源站 ip，在接入安全盾后需要对源站进行白名单限制；
- **无解析域名访问能力：**安全盾完全绕过了 DNS 带来的诸多麻烦，比如 DNS 劫持、

DNS 更新生效慢、DNS 解析不准确、DNS 洪水攻击、域名被封等等；

- **真实 IP 透传到源站：**通过源站安装插件，能够实现在源站获取真实访问者 ip 的需求，最大程度保证安全盾与客户业务的兼容性；
- **去中心化的节点选择算法：**终端根据网络最快原则进行安全网关的选择，没有中心化节点，可有效防御网络攻击。
- **兼容稳定且功能丰富的 SDK：**提供 windows、安卓、IOS 等多版本的 SDK
- **精准的 CC 攻击防护：**基于 SDK 和安全网关的配合能够让您的游戏彻底免疫 CC 攻击，且安全网关能够横向扩容。

3. 产品优势

3.1. 与传统高防产品对比

功能对比	安全盾	传统高防
DDoS 防御能力	无上限	有上限
入侵防御能力	0 误封，0 漏封	依靠策略规则，存在误封漏封
CC 防御	彻底免疫 CC 攻击	只能被动防御 CC 攻击
DNS 问题	规避各类 DNS 问题	存在 DNS 劫持、DNS 更新生效时间慢、DNS 解析不准确、DNS 洪水攻击、域名被封等问题
身份验证/链路加密	数据报文全链路加密，身份验证，防黑客破解，端到端的加密，APP 安全接入	传统清洗机房仅靠硬件设备来识别，无法解码私有协议
客户端体验	具备故障检测和无感知切换功能，不卡顿不掉线	攻击容易引起客户端掉线，造成业务不可用
APP 加速	根据智能算法选择延迟最低丢包率为 0 的节点，实现加速通信	根据 DNS 解析结果选择节点，存在不准确解析导致访问变慢的情况
加密通信	在原有业务基础上实现端	无额外加密方式，只能依靠业务本

	到端全链路加密，彻底保障业务数据安全	身进行加密。
防护配置	无需配置防护策略，一次接入，终身免疫	需根据攻击特征调整防护策略
防护成本	防护成本很低	防护成本很高
调度能力	秒级调度，快速切换节点	调度时间很长

3.2. 与其他安全盾产品优势对比

- **资源优势：**其他竞品一般采用公有云节点作为盾机网关，成本低但是容易被打穿，智安安全盾均具备百 G 到千 G 的防护能力，更具防护能力；
- **KEY 热更：**其他竞品一般不支持 KEY 热更，智安安全盾支持；
- **SDK 绕过：**其他竞品一般不支持 SDK 绕过，智安安全盾支持；
- **真实 IP 透传：**其他竞品获取真实访问 ip 需要安装 agent，智安安全盾不需要；
- **代码审计：**其他竞品一般不支持 SDK 代码审计，智安安全盾支持；
- **定制化：**其他竞品一般不支持定制化和私有化，智安安全盾支持。

4. 客户案例

4.1. 成都某游戏公司

项目背景：客户的网络游戏客户分布在全球各地，需要实现全球网络加速和安全防护，同时满足全球用户的游戏服务。目前存在的问题，包括：

① 游戏经常遭受 DDoS/CC 攻击，导致部分游戏大区瘫痪；

② 游戏后台经常遭遇恶意扫描和入侵攻击；

③ 部分地区和国家访问游戏体验不佳。

客户需求：实现全球用户的加速访问并有效防御各种网络攻击。

整改方案：

① 部署国内多线高防节点，实现国内用户的就近接入；

② 部署海外 anycast 节点，实现海外用户的就近接入；

③ 通过零信任控制中心实现终端设备、访问连接的合法性认证；

④ 取消业务域名的解析，对源站进行白名单访问限制，实现源站的完全隐身。

4.2. 株洲某工业龙头企业

项目背景：客户的服务器放在企业内网，但是有内网 APP 访问和外网 APP 访问需求，其中，外网 APP 使用的域名解析到互联网出口的负载均衡设备 IP，再通过 NAT 转发到内网服务器。存在一定的安全风险，包括：

① 服务器公网 IP 遭受 DDoS/CC 攻击，导致出口带宽饱和，影响整个企业业务；

② 内网 APP 系统存在入侵风险；

③ 公网 IP 暴露导致其他业务公网 IP 暴露。

客户需求：

① 终端设备管理和授权访问；

② 完全隐藏公司公网 ip；

③ 实现业务系统的远程安全访问。

解决方案：

① APP 终端集成安全盾的 sdk，包括 Android 和 ios；

② Web 端使用集成了安全盾 sdk 的定制浏览器(也叫 web 盾)进行业务访问，包括 PC 和 MAC；

③ 建立内网 Gateway：用于认证内网 sdk 数据，并将业务数据转发至 proxy；

④ 建立内网 Proxy：用于发起对源站的请求；

⑤ 建立负载均衡：用于映射 proxy 的内网地址到公网；

⑥ 建立公网 Gateway：用于认证公网 sdk 数据，并将业务数据转发至 proxy；

5. 关于我们

深圳市智安网络有限公司（简称：智安网络）是深圳市高新技术企业，下设成都智安云御网络有限公司（安全运营中心）和深圳市智安网络有限公司南京分公司（研发中心）两个子公司，成立于 2017 年 12 月 27 日，注册资本 2,000 万(元)。

作为安全运营中心，成都智安云御网络有限公司（简称：智安云御）成立于 2021 年 3 月，智安云御立足四川，放眼全球，坚持用户需求为导向，安全合规为目标，自主研发为宗旨，力争成为云安全领域领先者，在数字时代为用户的云安全及数据安全保驾护航。

智安云御基于企业安全能力模型 IPDRC（风险识别、安全防御、安全检测与响应、安全管控）构建安全 API 即服务的能力，搭建了智安安全中台。通过该中台，衍生了 6 条产品线路，形成“云 X 系列”的产品服务体系。

智安云御产品体系有：**云检**（流量检测--基于 snmp 与 flow 流量分析协议实现流量的采集、归类、威胁识别与告警）、**云测**（安全测试--提供可用性、漏洞、基线、权限、内容方面的风险测试和体检报告）、**云防**（攻击防御--提供主机/容器安全防护 cwpp 和网站/APP 安全防护 waap 能力）、**云控**（访问控制--基于零信任 SDP 与 IAM 理念实现下一代 VPN 技术）、**云保**（等保整改---一站式等保 2.0 建设服务平台）、**云密**（密码整改---一站式商用密码建设服务平台）