2023

智安网络

ZHIAN NETWORK

云墙-网站综合防御系统

技术白皮书

AQ-CP-050 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. 背景概述

随着计算及业务逐渐向数据中心高度集中发展，Web 业务平台已经在各类政府、企业机构的核心业务区域，如电子政务、电子商务、运营商的增值业务等中得到广泛应用，很多企业都将应用架设在 Web 平台上，Web 成为一种普适平台。

Web 业务的迅速发展也引起了黑客们的强烈关注，他们将注意力从以往对传统网络服务器的攻击逐步转移到了对 Web 业务的攻击上。黑客利用网站操作系统的漏洞和 Web 程序的 SQL 注入漏洞等得到 Web 服务器的控制权限，轻则篡改网页内容，重则窃取重要内部数据，更为严重的则是在网页中植入恶意代码，使得网站访问者受到侵害。

当前网络上 75%的攻击是针对 Web 应用的。这些攻击可能导致网站遭受声誉损失、经济损失甚至政治影响。各类网站客户已逐渐意识到 Web 安全问题的重要性，但传统安全设备(防火墙/IPS)解决 Web 应用安全问题存在局限性，而整改网站代码需要付出较高代价从而变得较难实现。同时，很多关系国计民生的重要网站，面临监管机构安全合规的要求。

1.2. 传统防火墙可否抵抗 WEB 攻击？

防火墙作为一款历史悠久的经典产品，在 IP/ 端口的网络时代，发挥了巨大的作用：合理的分开了安全域，有效的阻止了外部的网络攻击。防火墙在设计时的针对性，在当时显然是网络安全的最正确选择。但在网络应用高速发展，网络规划复杂化的今天防火墙的不适应性就越发明显，从用户对网络安全建设的需求来看，传统防火墙存在以下问题：

传统防火墙鉴于 IP/端口，无法对 WEB 应用层进行辨别与控制，无法确定哪些 WEB 应用经过了防火墙，自然就谈不上对各类威胁进行有效防守了。面对 WEB 应用层的攻击，防火墙显得力所不及，无法检测或拦截嵌入到普通流量中的恶意攻击代码，比

方病毒、蠕虫、木马等。

传统防火墙无法抵抗来自 WEB 应用层的威胁，自然就无法提供给用户有效的安全策略拟订依据。传统防火墙的防守能力有限致使了用户对内网服务器的安全状态没有直观的体现和把握，缺乏安全信息的可视化。

1.3. 入侵检测系统（IDS） 可否抵抗 WEB 攻击？

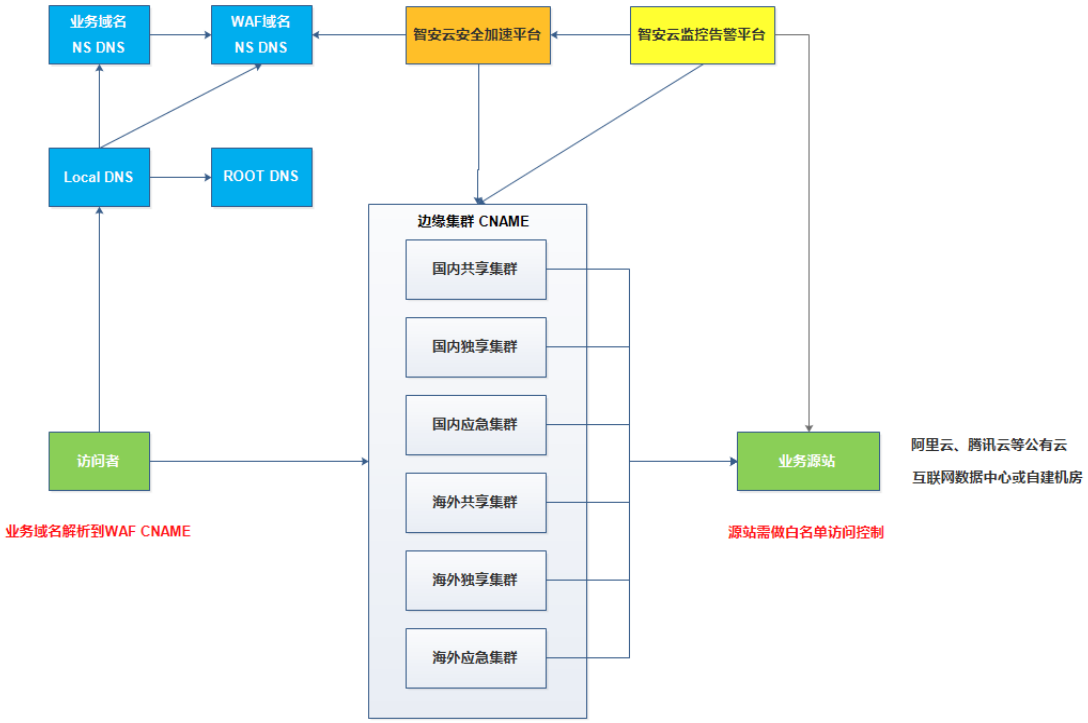
入侵检测系统（IDS）使用特征识别技术记录并报警潜在的威胁。其工作模式是被动的，它不能阻止攻击，也不能对未知的攻击进行报警。目前大多数攻击特征数据库都是网络层的攻击，此外，可以通过加密，TCP 碎片攻击以及其他方式绕过入侵检测系统的防御。

1.4. 入侵防御系统（IPS）可否抵抗 WEB 攻击？

IPS 只能针对操作系统和应用软件的底层破绽进行防备，缺乏针对 Web 攻击威胁的防守能力，对 Web 攻击防备效果不佳。缺乏攻击过后防备体制，不具备数据的双向内容检测能力，对未知攻击产生的结果无能为力，如入侵防守设施无法应付来自于 web 网页上的 SQL，XSS 破绽，无法防守来自内网的敏感信息泄露或许敏感文件过滤等等。

2. 平台介绍

智安网络云墙（网站综合防御系统），是一款集 DDoS 防御、CC 防御、WEB 入侵防御、网页防篡改、边缘计算、L4\L7 反向代理、CDN 加速、智能 DNS 解析、SSL 管理、IPV6 功能于一体的网站综合防御平台，支持边缘节点集群化部署和扩容，支持在信创软硬件环境运行，支持自定义 WAF 规则和国家地区封锁。平台可衍生三种典型的安全解决方案：面向 DDoS 攻击防御（智云堤）、面向 WEB 防入侵（智云墙）、面向网络加速（智云速）。



3. 平台功能

3.1. WEB 入侵防御

对 Web 流量进行深度检测，对 Web 应用进行深度防护，提供全面的入侵防御能力。能在攻击到达 Web 服务器之前进行有效阻断，防止恶意的请求或内置非法程序的请求访问目标应用。能解码所有进入的请求，检查这些请求是否合法合规；仅允许正确的格式或 RFC 遵从的请求通过。已知的恶意请求将被阻断，非法植入到 Header、Form 和 URL 中的脚本将被阻止。平台还能进行 Web 地址翻译、请求限制、URL 格式定义及 Cookie 安全，支持防御以下常见威胁：SQL 注入、跨站脚本攻击、Webshell 上传、后门隔离保护、命令注入、非法 HTTP 协议请求、常见 Web 服务器漏洞攻击、核心文件非授权访问、路径穿越、扫描防护等。

3.2. CC 恶意攻击防护

对单一源 IP 的访问频率进行控制，基于重定向跳转验证，人机识别等。

针对海量慢速请求攻击，根据统计响应码及 URL 请求分布、异常 Referer 及 User-Agent 特征识别，结合网站精准防护规则进行综合防护。

3.3. 流量型 DDOS 防护

智能联动全网高防节点共同为业务提供云清洗服务的资源，具备全方位的 DDoS 防护功能，完美防御 SYN flood 攻击 、ICMP flood 攻击、UDP flood 攻击、Ak flood 攻 击、等 DDoS 攻击，确保流向客户的流量均为安全、正确的业务流量。

3.4. 高级 WEB 应用安全防护

支持多种端口：支持除 80 和 443 以外的非标端口的防御需求。

扫描器爬虫防护：自定义扫描器与爬虫规则，用于阻断非授权的网页爬取行为，添加定制的恶意爬虫、扫描器特征，使爬虫防护更精准。

网页防篡改：对网站的静态网页进行缓存配置，当用户访问时返回给用户缓存的正常页面，并随机检测网页是否被篡改。

网站反爬虫：动态分析网站业务模型，结合人机识别技术和数据风控手段，精准识 别爬虫行为。

误报屏蔽：针对特定请求忽略某些攻击检测规则，用于处理误报事件。

隐私屏蔽：避免在防护事件日志中，出现用户名或者密码等敏感信息。

防敏感信息泄露：防止在页面中泄露用户的敏感信息，例如：用户的身份证号码、 手机号码、电子邮箱等。

3.5. 安全监控

实现基于安全事件级别的安全监控，通过对安全日志分析、攻击者追踪等手段，将具有危害的行为、需要处理的事件进行可视化展示，实现高效管理。

完整的记录攻击事件的各种元素，方便客户分析和了解攻击状态。能够对 HTTP/HTTPS 流量进行解析，可以有效的识别并且能够完整记录 HTTP 请求头部、请求内容、响应头部、响应内容。

3.6. 网站隐身

Web 攻击往往由探测网络漏洞开始，在网络上很容易找到漏洞扫描工具对一个网站的应用程序、服务器、URL 等进行扫描。智安网络云安全加速平台完全隐藏站点地址，黑客将无法查看 Web 的源信息,避免其绕过平台直接攻击 Web 源站。

3.7. CDN 缓存加速

为了提高被保护系统的访问速度同时消除 WAF 过滤分析过程中带来的延时，平台提供了 CDN 缓存加速功能：通过内存缓存、内容压缩、文件转码和相关算法及管理相关的静态内容，一旦有用户访问，客户端直接通过 WAF 缓存中获取，避免了用户重复通过 Web 服务器并进行协议解析等相关操作，从而加快了访问速度，减轻了 Web 服务器的负担。

3.8. 安全策略配置

平台提供了默认的安全策略对 Web 网站或应用进行严格的保护。除了默认的策略外，用户还可以创建客户化的策略。

支持黑白名单的配置，可以设定可信的访问客户端 IP（白名单）而不受安全策略规则的检测；设定非法的访问客户端（黑名单），直接禁止其任何对 WEB 服务器的访问。

支持用户自定义规则库，内置丰富的策略配置项，可根据自身业务特点灵活制定精细化防护规则，满足专业安全需求。提供自定义规则配置功能，客户可针对自身使用和需求定制符合自己环境的防御策略，防御更精准，并有选择地进行启用和停用操作。

3.9. 观察和防御模式

用户自定义新增了某个不当的规则可能影响当前应用的正常使用。云安全平台提供了观察和防御两种模式，在观察模式下，所有安全策略规则都只是对应用流量数据包进行检测并记录，而不做任何阻断功能；在防御模式下，所有的安全策略规则可根据单条规则的配置来制定阻断措施。

3.10. 行为审计

平台详尽的记录并统计用户对 Web 应用资源的访问，包括客户端地址、客户端类型、资源地址、请求方式、访问流量、访问时间等信息，实现有效的用户行为跟踪和访问统计分析。生成基于地区区域的访问统计，便于识别 Web 应用的访问群体是否符合预期，为应用优化提供指导。

平台详细记录所有攻击行为，对攻击来源、数据、时间、处理结果形成详细的统计数据，便于查看应用的攻击态势。

3.11. SSL 证书管理

提供 SSL 证书上传、申请、监控、自动续期服务，实现高强度双向加密传输，支持加密算法的自定义，防止传输数据被泄露或篡改。

3.12. 高可用性

以集群的方式提供服务，多台机器负载均衡，支持多种负载均衡策略。可多区域多集群的方式部署节点，避免了单点故障。

支持横向扩容，根据实际流量情况，增加或缩减集群节点，进行服务能力的弹性扩容。

4. 解决方案

4.1. 智云堤（DDoS 防护）

4.1.1. 【产品描述】

智云堤（DDoS 防护）是由智安网络云安全加速平台+DDoS 高防资源构成，云安全加速平台通过反向代理或端口转发的方式，将客户的业务域名或 IP 进行引流至 DDoS 高防集群，所有公网流量将优先经过高防集群，攻击流量将在高防清洗中心进行清洗过滤，并将正常访问流量转发到业务源站服务器。

DDoS 防护使用四层和七层转发的接入方式，支持 TCP/UDP/HTTP(S)/Websocket(s)等协议转发，支持全范围端口转发，支持共享集群和独享集群，支持国内集群和海外集群。

4.1.1. 【应用场景】

- **网站类 DDoS 攻击：** WEB 业务一直是 DDoS 攻击的重灾区，攻击者探测出站点服务的源站 IP 后，对服务器发起攻击，可以轻易的让网站瘫痪，无法正常运行。使用智云堤 DDoS 防护产品，对各种大流量 DDoS 攻击、洪水攻击等能秒级响应，快速有效解决被攻击情况，确保网站正常运行。适合：电商、政府、企业门户网站等。
- **游戏类 DDoS 攻击：**游戏行业现在面临的 DDoS 攻击是非常严峻的，对游戏服务器的拒绝服务攻击，大并发的请求拖垮服务器。一旦受到攻击将会导致用户无法登录、游戏延迟等问题，对游戏用户造成非常不好的影响甚至放弃这款游戏。使用智云堤 DDoS 防护产品，基于域名或者 IP 形式防御，系统自动检测并清洗针对游戏业务端口的各种类型洪水攻击，自动过滤有威胁的请求源，从而保障游戏业务正常运行。

4.1.2. 【产品优势】

- **高可用服务：**全自动检测和攻击策略匹配，实时防护；业务流量采用集群分发，性能高，时延低，稳定性好。
- **丰富的防护报表：**提供多维度统计报表，通过查看流量信息，了解当前网络安全状态。
- **海量清洗带宽：**拥有多线 BGP 防护带宽，轻松抵御 DDoS 攻击，可以满足活动大促、活动上线等重要业务的安全稳定性保障需求。
- **全方位多层防护：**弹性公网 IP、云服务器、负载均衡等云资源全方位防护，实时监测网络流量，发现攻击立即清洗。有效解决 SYN Flood/ACK Flood/ICMP Flood/UDP Flood 等多种网络层 DDoS 攻击。
- **全业务支持：**DDoS 高防 IP 服务支持网站和非网站业务，覆盖金融、电商、游戏、政府等各类业务，充分满足用户不同业务的安全防护需求。
- **专业运营团队：**7*24 小时运营团队随时应对；专业的运营人员随时解答您的疑问，为您的业务保驾护航。

4.1.3. 【接入流程】

登录智安云安全加速平台，配置回源规则，将业务的 DNS 域名解析或业务 IP 指向 DDoS 高防实例 IP 或 CNAME 即可。

4.1.4. 【计费方式】

计费项	计费模式	付费说明
防护能力	包年包月	提供的 DDoS 防护能力
域名/IP 数	包年包月	需要防护的域名（一级域名/二级域名）或 IP 数
业务带宽	包年包月	A.业务带宽限制是针对业务 IN 方向（高防回源流量）和业务 OUT 方向（高防

		出流量），业务带宽规格需要大于业务 IN 和业务 OUT 中最大流量值。 B. 当业务带宽不够用或业务 QPS 需要更高时，请及时升级，否则可能会导致丢包或者影响业务。

4.2. 智云墙（Web 应用防火墙）

4.2.1. 【产品描述】

智云墙（Web 应用防火墙）是由智安网络云安全加速平台+智安云安全团队构成，通过对 HTTP(S)请求进行检测，识别并阻断 SQL 注入、跨站脚本攻击、网页木马上传、命令/代码注入、文件包含、敏感文件访问、第三方应用漏洞攻击、CC 攻击、恶意爬虫扫描、跨站请求伪造等攻击，保护 Web 服务安全稳定。

4.2.2. 【应用场景】

- **网站日常 WEB 防护：**适用于金融、电商、o2o、互联网+、游戏、政府、保险等行业各类网站的 Web 应用安全防护。
- **电商抢购秒杀防护：**当业务举办定时抢购秒杀活动时，业务接口可能在短时间承担大量的恶意请求。Web 应用防火墙可以灵活设置 CC 攻击防护的限速策略，能够保证业务服务不会因大量的并发访问而崩溃，同时尽可能地给正常用户提供业务服务。
- **0Day 漏洞爆发防范：**当第三方 Web 框架、插件爆出高危漏洞，业务无法快速升级修复，Web 应用防火墙会第一时间升级预置防护规则，保障业务安全稳定。WAF 相当于第三方网络架构加了一层保护膜，和直接修复第三方架构的漏洞相比，WAF 创建的规则能更快的遏制住风险。

- **防数据泄露:**恶意访问者通过 SQL 注入，网页木马等攻击手段，入侵网站数据库，窃取业务数据或其他敏感信息。用户可通过 Web 应用防火墙配置防数据泄露规则。
- **防网页篡改：**攻击者利用黑客技术，在网站服务器上留下后门或篡改网页内容，造成经济损失或带来负面影响，用户可通过 Web 应用防火墙配置相应规则，在黑客发起恶意代码注入时，WAF 可实时检测并进行拦截，保证网页不被篡改。

4.2.3. 【产品优势】

- **可靠性：**通过防护集群作用，避免单点故障和冗余，并且支持横向扩容，可根据实际流量情况，缩减或增加集群服务器的数量，进行服务能力弹性扩容。
- **简易性：**30 分钟内部署和激活。
- **事件可追溯：**完整的记录攻击事件的各种元素，方便客户分析和了解攻击状态。
- **专业运营团队：**7*24 小时运营团队随时应对；专业的运营人员随时解答您的疑问，为您的业务保驾护航。

4.2.1. 【接入流程】

登录智安云安全加速平台，选购对应的 WAF 资源，配置回源规则，获得 CNAME 并更换业务域名解析为 CNAME，完成接入。

4.2.2. 【计费方式】

计费项	计费模式	付费说明
防护域名数	包年包月	支持防护的域名数（一级域名/二级域名）
业务带宽	包年包月	A.业务带宽限制是针对业务 IN 方向（高防回源流量）和业务 OUT 方向（高防出流量），业务带宽规格需要大于业务 IN 和业务 OUT 中最大流量值。

		B. 当业务带宽不够用或业务 QPS 需要更高时，请及时升级，否则可能会导致丢包或者影响业务。

4.3. 智云速（网络加速）

4.3.1. 【产品描述】

智云速（网络加速）是由智安网络云安全加速平台+全球加速资源构成，依靠全球节点之间的高速通道、转发集群及智能路由技术，实现各地用户的就近接入，通过高速通道直达源站区域，帮助业务解决全球用户访问卡顿或者延迟过高的问题。

4.3.2. 【应用场景】

- **游戏加速：**游戏行业面临延迟大、丢包多、掉线频繁等问题，严重影响终端用户的游戏体验。可以通过全球加速使游戏请求就近接入智云速，通过智云速的内网到达游戏服务器，极大地缩短了公网传输路径，减少延时、抖动、丢包等网络问题，提升游戏服务体验。
- **回国访问加速：**源站部署在海外，用户在国内的访问业务，往往会因为区域之间的网络状况不同而导致延时和丢包率增加，影响访问业务的用户体验。通过智云速可有效降低网络时延和丢包率，保障网络的快速和稳定性，提升用户体验。
- **其他出海业务加速：**跨国网站、跨境电商、全球运营类 App、全球化直播、视频，全球金融等。

4.3.3. 【产品优势】

- **超低延迟：**回国延迟可低至 30ms，快速连接海外至国内，延迟极低。
- **高稳定性：**可用性 99.9%，高度冗余，主用线路故障智能切换备用线路。

- **轻载负荷：**全网利用率不超过 50%，丢包率低，速度稳定不拥挤。
- **支持突发：**通过动态资源调配,轻松满足带宽峰值需求。

4.3.4. 【接入流程】

登录智安云安全加速平台，配置回源规则，获得 CNAME 并更换业务域名解析为加速 CNAME，完成接入。

4.3.5. 【计费方式】

计费项	计费模式	付费说明
加速带宽	包年包月	A.加速带宽限制是针对业务 IN 方向（高防回源流量）和业务 OUT 方向（高防出流量），业务带宽规格需要大于业务 IN 和业务 OUT 中最大流量值。 B.当业务带宽不够用或业务 QPS 需要更高时，请及时升级，否则可能会导致丢包或者影响业 务。
域名数	包年包月	需要加速的域名数（一级域名/二级域名）

5. 客户案例

5.1. 成都某游戏公司

项目背景：客户经常受到来自黑客和同行恶意竞争者的 DDoS 攻击，严重影响玩家体验和游戏寿命。

整改方案：

1.通过采购智云堤（DDoS 防护）产品，提供 T 级多线 BGP 带宽资源，超大防护带宽，满足游戏客户的大流量攻击防御需求。

2.针对游戏业务特征，定制化 CC 防御策略，有效拦截 4-7 层恶意流量。

3.分布式清洗节点部署，近源接入防护，保障游戏业务的流畅稳定运行。

4.7x24 小时不间断监控，全天候管家式服务，保证业务不中断。

客户价值：为客户提供高可用、高可靠的防护服务，减少安全投入和运维成本，避免 DDoS 攻击带来的直接或间接经济损失。轻松接入，有效应对黑产、DDoS 攻击给业务带来的威胁问题，保障客户业务安全稳定运营。

5.2. 某大型证券公司

项目背景：该证券公司需要对外公布大量信息，如含金融政策、理财产品、网上银行等相关内容，一旦出现网页篡改、信息泄露等安全问题将会对金融企业和客户造成巨大的经济损失，因此需要做出相应安全防护措施。

解决方案：

1.通过采购智云墙（Web 应用防火墙）产品，将需要防护的网站配置在平台中。从而实现 Web 应用层的防护，包括了网页防篡改、SQL 注入、跨站脚本攻击等常见 Web 攻

击。

2.7X24 小时监控所有的网站，当 web 攻击及可用性问题时第一时间发出告警警报给管理员，防止影响面扩大，实现对 web 攻击的快速响应，有效提升运维效率。

3.通过可视化的风险报表及 web 攻击的一键封堵提升安全运维效率。

客户价值：通过内置的丰富规则库，避免用户网站被劫持、挂马、植入后门、篡改；通过 7*24 小时的应急处置服务，提升企业安全事件快速响应能力，满足监管部门合规要求；

5.3.某海外电商公司

项目背景：该电商公司业务系统部署在海外，服务的客户群体主要是在国内。由于国内客户直接访问海外源站会出现延迟较高或丢包率高的情况。因此该公司需要一套让国内客户顺畅访问其海外电商平台的解决方案

解决方案：

1. 通过采购智云速（网络加速）产品，将需要加速的网站配置在平台中。
2. 为该公司提供优质的 CN2 线路或亚太 BGP 线路
3. 配备多节点资源，避免单点故障

客户价值：提升了网站的访问速度，提高用户的体验感。减少源站带宽成本，隐藏源站 IP 增加安全性，同时增加内容可用性和冗余。对网络进行全方位的监控，及早发现问题、预防问题和处理问题。

6. 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）