网络与通信安全

信舷WEB应用防火墙系统【AISWAF】

需求背景

Web 服务被普遍认为是新一代应用程序集成以及通向新的商业模式的大门，是企业对外发布数据和与其他企业相互联系的重要途径，这种情况下，如何保证 Web 应用的安全问题就变成信息安全的头等大事。Web 应用的安全非常复杂，因为 HTTP 协议的灵活性，这就导致在 HTTP 之上的各种应用都有自己独特的特点，同时由于用户访问应用的方式千差万别，这就导致了 Web 应用的安全是一个需要很高的技术含量、可以适应用户不同应用的专业安全设备。所以如果想全面地实现 Web 应用的安全，有效的方法就是部署专业的 Web 应用防火墙（WAF）产品。

产品介绍

亚信安全 WEB 应用防火墙系统【AISWAF 】提供了针对最新应用程序攻击的自动化防护，例如 SQL 注入、XSS、CSRF、路径遍历以及更多攻击。亚信安全 WEB 应用防火墙系统融合了自动化的应用程序学习和来自应用程序防护中心的最新保护策略与特征码，能够准确地识别出攻击并加以阻止；加上高粒度的关联规则、基于声誉的安全以及强大的报告框架，为您提供了一套优秀的多级别保护。亚信安全 WEB 应用防火墙系统可以提供透明桥、反向代理、嗅探模式多种部署方式，领先的透明部署模式具备万兆级别的数据处理性能、低于一毫秒的延时以及高可用性选择，能够满足大规模数据中心的建设要求。

优势

精准防护复杂场景

细颗粒度的自定义规则，提供超过40个HTTP 相关的策略条件，用户可以任意组合策略条件以应对多业务、多场景的精细化防护需求。

业务无感知接入

基于透明检测技术实现二层透传，无需改变网络结构及数据包，在不追加额外性能损耗的情况下，完成WAF接入和交付。

自适应敏捷应用发布

基于AI和机器学习建立动态模型，能够适应Web应用程序的结构和流量的快速变化，从而实现WAF策略的自动化校准，支持更快的应用发布周期。

多维关联有效降低误报率

基于关联分析引擎对攻击进行多维度分析，包括协议校验、特征签名、应用模型、威胁情报等，精准识别并拦截恶意攻击。

降低安全团队运维压力

基于智能告警聚合和攻击回溯功能，为安全运营团队提供快速诊断相似性攻击和详尽取证信息的能力。

卓越的处理性能

一个单独的WAF网关就可满足大型企业的需求，也可以扩展出多个统一管理平台下的网关集群。

功能

- 动态建模和自动策略
- 多层次的防护及关联
- 强大的安全策略设置
- 应用用户跟踪
- 灵活的告警分析
- 集中化管理
- 应用防护中心（ADC）
- Web 应用层面的 DDoS 防护
- 侦测零日漏洞
- 敏感信息防泄露
- 机器人访问抑制
- 潜伏式隐蔽攻击防护
- API 安全防护

应用场景

敏感数据防泄漏：避免因黑客的入侵攻击，导致网站核心数据被窃取。

防御 CC 攻击：缓解黑客控制大量主机恶意访问服务器，导致 Web 服务器资源耗尽。

0day 漏洞修复：有效侦测 0day 漏洞攻击，并提供快速修复的规则策略。

网页应用保护：社交攻击、技术攻击、业务流程攻击等各个方面防护网页应用。

网站内容爬取防护：识别网页爬取和恶意评论信息，精准阻止针对网页内容的恶意行为。

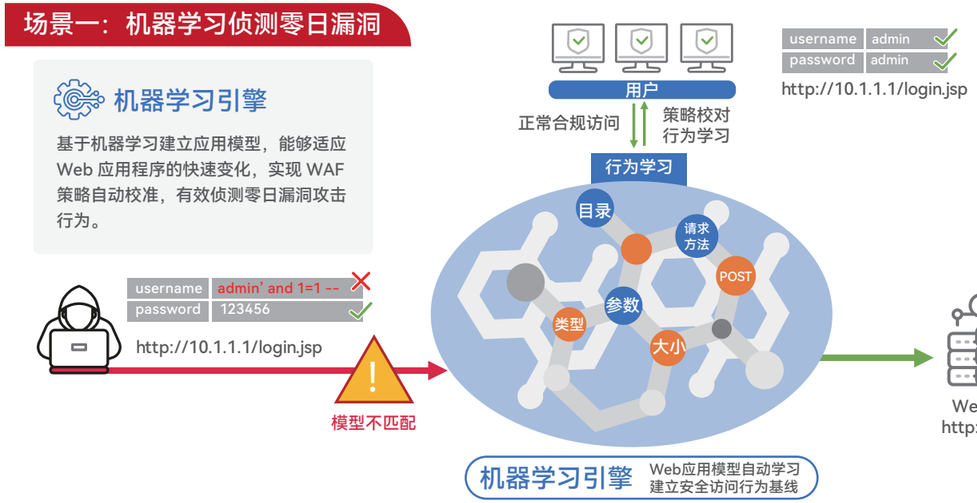
机器人管理和抑制：识别机器人的内容抓取、账号欺诈等行为，防止访问延迟增加和运营分析失真。

API 安全防护：将 API 的请求引流到 AISWAF，分析和监控 AISWAF 上的 API 流量。

场景一：机器学习侦测零日漏洞

机器学习引擎

基于机器学习建立应用模型，能够适应 Web 应用程序的快速变化，实现 WAF 策略自动校准，有效侦测零日漏洞攻击行为。



场景二：敏感数据防泄漏