



# 优炫网站应用防火墙系统 产品介绍

北京优炫软件股份有限公司

版权所有 侵权必究

# 目 录

1	产品概述 .....	1
2	产品特点 .....	2
3	功能特性 .....	3
4	亮点功能 .....	1
5	产品部署 .....	2
5.1	透明桥模式 .....	2
5.2	反向代理 .....	2
5.3	镜像模式 .....	2
5.4	云部署 .....	3

# 1 产品概述



图 2U 设备外观示意图

优炫网站应用防火墙系统（UXSINO Web Application Firewall，简称 UX-WAF）是北京优炫软件股份有限公司结合多年在应用安全领域理论研究及攻防实践经验积累的基础上，自主研发的新一代应用级综合防护系统。保护您的 WEB 网站免受众多已知或未知的应用层攻击，诸如 SQL 注入、XSS 跨站、木马上传、CC 攻击等。优炫网站应用防火墙系统能够帮助用户解决目前所面临的各类常见及最新的应用安全问题，同时满足等级保护、行业规范等政策法规的安全建设要求。

优炫网站应用防火墙系统拥有多种不同硬件型号，充分满足各种类型客户需求，提高 WEB 业务的可用性和安全性，确保 WEB 业务能够快速、安全、可靠地运行。

## 2 产品特点

- 强大的攻防能力

- 多年安全策略积累，专业安全团队，规则误报率低。
- Web 0day 漏洞补丁 24 小时内全国同步。
- OWASP TOP10 精确防护，智能攻击者锁定，智能补丁，驱动防篡改，全方位防护网站安全。

- 高效的处理性能

- 插件式的高效策略处理引擎。
- 性能与规则数量无关，高性能不牺牲安全。

- 简单的应用部署

- 透明部署、即插即用。
- 站点自动发现，降低配置复杂度。
- 配置变更平滑，安全应用不影响客户业务。

- 增值的核心功能

- 实时对 http 站点进行 https 加密与防护。
- 智能防护，实时封锁恶意攻击者。
- 智能学习，智能学习站点特征，定制防护策略。
- IPV6 站点防护支持。

## 3 功能特性

### ● 深度防御

- 1) 对 HTTP/HTTPS 流量解析，全方位检查网络中的攻击。
- 2) 依据 HTTP 协议和 WEB 应用相关协议规范，对 WEB 应用的访问请求和应答进行深入分析和细粒度检查，阻止常见的 WEB 攻击。
- 3) 高效的内容解析引擎对访问数据流进行协议检查，可屏蔽服务器指纹探测、阻断扫描、防止服务器敏感信息泄露。
- 4) 对能够“绕过”传统防火墙与 IPS 的攻击方法和手段，可以精确地阻断。
- 5) 智能学习、分析应用业务流程和用户访问流程，构建主动防御模型，杜绝未知攻击及合法用户的非法操作。
- 6) 整理、分析、分类网站攻击特征，对网络中的流量进行攻击判断。
- 7) 对访问来源或者访问资源进行单点控制，避免超出阈值的流量到达 WEB 服务器。

### ● 2、高可用性

- 1) 软件 BYPASS，避免由于产品性能问题而影响用户网络中的业务。
- 2) 硬件 BYPASS，避免由于产品硬件故障导致用户的网络不可用。
- 3) 双机热备，确保主设备故障下备机接管网络安全防护工作。

### ● 3、用户交互

- 1) 系统的操作流程简单，符合人性化设计。
- 2) 分类记录攻击行为后形成详细的统计及 24 小时攻击趋势列表。
- 3) 审计报表为系统的安全审计提供详细的数据，为管理者提供可靠的决策依据，降低应用系统的管理维护复杂度。
- 4) 支持 SYSLOG 日志服务器、SNMP 服务器、邮件服务器对攻击日志和运行日志的采集。

## 4 亮点功能

- 虚拟化 WAF 可运行于多种虚拟化平台，如 VMware、KVM、Xen。
- 云 WAF 支持，很好的兼容 OpenStack 等多种云平台。
- 拥有防撞库、防刷票等业务针对性的安全功能模块。
- 负载均衡功能，可将连接请求按需求分配到服务器集群中，确保重负载情况下服务器快速响应。
- 智能补丁功能，可为扫描器发现的 WEB 服务漏洞进行结果导入，为被保护的 WEB 服务器打虚拟补丁。
- 支持 8000+条 SQL 注入防护规则，检测效果经过严格检验。

## 5 产品部署

### 5.1 透明桥模式

透明桥模式下，业务口工作在桥接口下，用户无需改变网络中拓扑，将 UX-WAF 串联到网络中即可，达到即插即用就能实现保护 WEB 服务器的效果。在桥模式下，支持双机备份，包括主备模式和主主模式；支持软件 BYPASS 和硬件 BYPASS，具备高可用性。



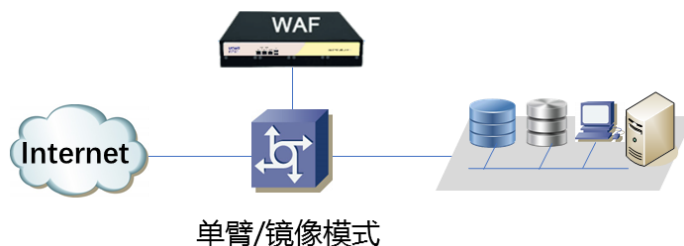
### 5.2 反向代理

反向代理模式和单臂模式实现原理相同，不同的是反向代理模式使用两个业务接口，而单臂模式只使用一个业务接口。

在反向代理模式下，用户需要改变原有拓扑模型，客户端访问的目的地址是 UX-WAF 代理的接口 IP，UX-WAF 再将访问请求转发到后台服务器，此模式可以隐藏服务器的真实 IP 地址，在反向代理模式下，也支持双机热备，包括主备模式和主主模式；并且具备服务器存活探测功能，可以根据特定算法实现负载均衡，用以保障服务器业务的连续性和连通性。

### 5.3 镜像模式

UX-WAF 不串联到网络环境中，而是旁挂在交换机设备上，通过流量镜像方式对网络中的流量进行检测和告警。其部署方式与 IDS 相似。



## 5.4 云部署

UX-WAF 支持云部署方式，如 OpenStack 部署或其他第三方运营管理平台。

