天融信 Web 应用安全防护系统

1 产品概述

天融信 Web 应用安全防护系统（TopWAF）是天融信凭借多年的网络安全研究经验开发的具有完全自主知识产权的一款专门为 Web 应用提供防护的安全产品。

TopWAF 通过内置上千条由天融信阿尔法攻防实验室提供的安全规则，对从客户到网站服务器的访问流量和从网站服务器到客户的响应流量进行双向安全过滤，来提供 WEB 应用攻击防护、DDOS 防御、URL 访问控制、网页防篡改等功能，能够有效的抵御针对 Web 应用的攻击而导致的网站被恶意篡改、敏感信息泄露、网站服务器被控制等事件的发生。是适用于政府、企业、高校以及运营商的可信的防御 Web 威胁的安全产品。

2 产品特点

2.1 先进的全并行安全系统

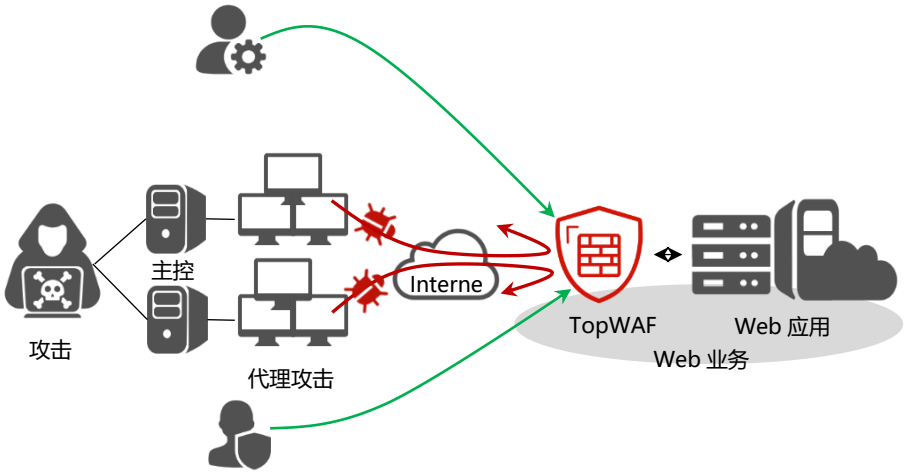
TopWAF 基于天融信 NGTOS 64 位安全操作系统，NGTOS 安全操作系统采用了先进的多路多核架构。NGTOS 使用了兼容 TCP/IP 特性的用户态的协议栈，且避免了传统内核态协议栈在业务处理过程中操作系统上下文切换和内核空间到用户空间的数据拷贝，将系统效率推向极致。

2.2 精准的 Web 应用攻击防护

TopWAF 通过对 Web 应用流量双向深度检测，为 Web 应用提供精准、细致的攻击防护能力，阻止如 SQL 注入、XSS、CSRF 等攻击，有效应对 OWASP Top 10 定义的威胁及其变种。在请求方向，TopWAF 在攻击数据到达 Web 服务器之前，对请求重组、规范、解码，检查其合法性及合规性，防止恶意请求或者内置了恶意代码的请求访问 Web 应用。TopWAF 对输入的各种编码和字符集进行的全面标准化和归一化，有效防御各种编码及字符变形的攻击绕过。对于响应方向，TopWAF 隐藏 Web 站点源信息，如 HTTP 头信息、URL 返回码等，以延缓黑客攻击进展。除反向防护模型外，TopWAF 通过自学习双向数据（请求/响应）功能可以建立正向防护模型，智能应对未知威胁。此外，TopWAF 支持敏感信息防泄露，可对身份证、电话、银行卡及关键字等类型响应信息进行拦截，保护用户隐私和机密数据。

2.3 有效的应用层 DDoS 防御

相对于网络层 DDoS 攻击，应用层 DDoS 攻击可操作性更强，危害更大，现今应用层 DDoS 攻击已成为 Web 安全防护的一个重点方向。TopWAF 基于先进的源信誉检查机制，并根据长期流量模型学习结果和历史记录，动态感知恶意流量，有效防御各类型应用层 DDoS 攻击，如当前流行的 HTTP flood 、CC、慢速攻击等。TopWAF 可有效识别及阻断应用层 DDoS，确保 Web 服务器能为真实的用户提供服务，保证客户业务的连续性。

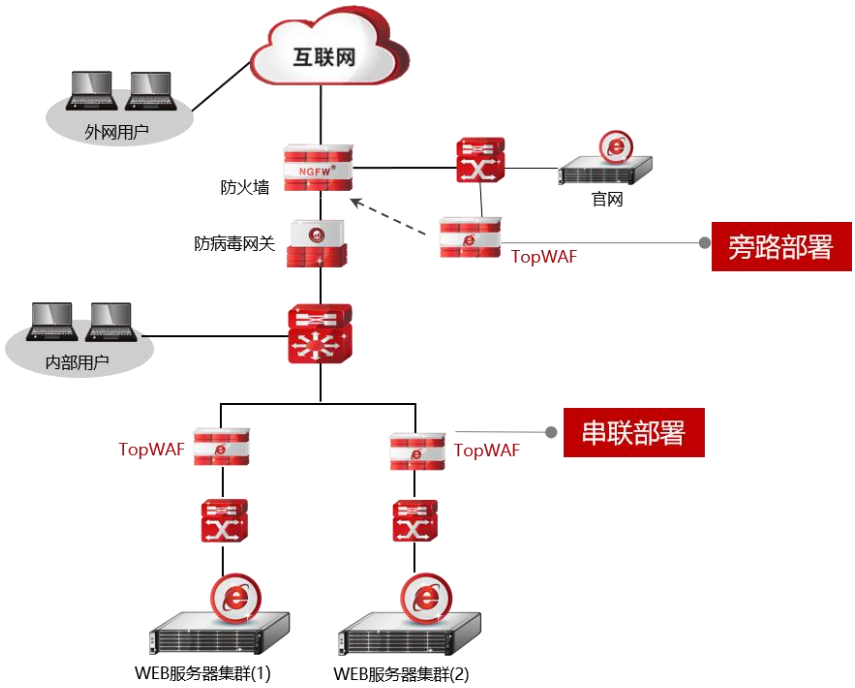


2.4 智能的网站行为分析

TopWAF 能够实时显示系统的运行情况，并直观展示网络中的攻击行为（包括：攻击参数信息、攻击类型、触发规则、攻击检测过程、篡改行为、DDOS 攻击信息等）来提供威胁统计功能，分析防护对象受到攻击信息，并显示在攻击事件列表中，同时生成攻击日志，通过 TopWAF 的日志报表就可以快速追踪攻击来源、网站漏洞等，保障网络安全。

3 典型应用

拓扑展示



客户收益

- 可以有效的防止因黑客攻击而造成的用户网站被恶意篡改、恶意仿冒、敏感信息被泄露、网站被远程控制、被信息安全主管单位漏洞通报等安全事件的发生。客户可以对自身网站安全情况了然于胸，提升用户对自身网站安全防护的信心。
- 可以通过对日志报表的分析，全面详细的了解自身网站遭受黑客攻击的状况。也可以通过 TopWAF 自带的 Web 漏洞扫描器功能对网站进行扫描检查，并根据扫描结果及时的组织网站开发人员、网站安全人员对网站漏洞进行修复，使得网站更加安全，发生网站安全事件的几率更低。
- 通过 TopWAF 对用户业务流量的负载展示，用户可以了解网站服务器的每秒事务数、并发连接数、吞吐率等网站性能参数，为其网站业务的调整提供参考依据。通过对网站访问情况的智能分析，管理员可以直观了解到网站的业务情况，并以此来作为网站业务调整的依据。
- TopWAF 的部署符合国家信息安全等级保护中对网站安全的要求。

4 功能列表

部署方式	支持串联部署、旁路监测模式部署、负载均衡模式部署、反向代理模式部署
网络适应性	支持 VLAN 划分，支持多 VLAN 环境下 trunk 的部署、物理接口支持子接口
IPV6 支持	支持 IPV4/IPV6 双栈，能够对 IPV6 进行细粒度的访问控制及全面的应用层防护。
HTTPS 支持	支持 HTTP/HTTPS 站点防护★
协议合规检查	支持请求限制配置通过定义最大请求头长度、最大 content-length、最大 body 长度、最大请求行长度、最大 header 行长度、最多 cookies 个数、最多 header 头个数、最大 header 长度等来对请用户数据做合规性检查
WEB 安全防护	能够识别和阻断 SQL 注入攻击,Cookie 注入攻击，命令注入攻击
	能够识别和阻断跨站脚本(XSS)攻击
	支持 webshell 等后门上传防护、支持对中国菜刀等工具对后门连接的阻断
	支持对 appscan、awvs 等扫描器的扫描防护
	支持远程文件包含、本地文件包含、目录遍历、信息泄露等攻击防护
	应能识别和阻断跨站请求伪造(CSRF)攻击
	支持对身份证、信用卡、手机电话号码、座机电话号码、邮箱地址等敏感信息做检查，当检查到此类数据后可通过配置特殊字符予以替换隐藏，防止信息泄露
	https 证书支持直接将证书内容填充到 waf 内使用，不用再上传或者转换证书使用
配置易用性	支持域名自学习，可以自动学习网络中网站服务器的 IP 地址及此地址下的域名
DDoS 攻击防护	支持基线学习，可以自动学习用户 http 正常流量阈值模型，并给出推荐阈值配置项
	对 DDoS 流量支持检测清洗和强制防御两种模式，检测清洗根据是否到达阈值对流量进行清洗，强制清洗对所有流量直接进行流量清洗判断
	支持针对每秒包数、每秒新建连接数、每秒并发连接数对 HTTP/HTTPS Flood 攻击做控制配置
	支持对 HTTP/HTTPS Flood 攻击做重定向或验证码验证，将异常流量加入黑名单
网页防篡改	网关型网页防篡改，无需在服务器中安装任何插件，可以对动态网 站及静态网站文件内容进行防篡改，当检测到篡改后可以实时恢复篡改内容
WEB 漏洞扫描	支持多种 WEB 应用漏洞的安全扫描检测，如 SQL 注入、跨站脚本、目录遍历等
负载均衡	支持多服务器的负载均衡，支持轮叫、加权轮叫、原地址散列、最小连接等多种负载均衡算法
网络数据分析	Web 界面可以直观查看 WAF 扩展卡、接口、USB 口、管理口、HA 口及业务口的运行状态
	可以实时查看设备并发连接数、每秒事务数及 HTTP 应用层吞吐率等数据并以可视化的方式展示
设备运行数据分析	可以实时查看设备 CPU、内存、硬盘等自身使用率情况
日志报表数据分析	日志支持以 syslog 和 welf 两种格式向远端日志服务器发送日志
	日志传输可加密，且管理员可以配置加密密码
	支持最近一小时、一天、三十天等多种条件内攻击源 IP 攻击次数及攻击分布 TOPN 的统计
系统管理	支持 SSL 的 WEB 界面、SSH、Console 多种方式管理
	支持操作系统 WEB 方式升级及命令行等方式的离线升级
	支持规则库的在线升级和离线升级
	支持攻击日志邮件告警，可以定时将特定攻击类型的攻击日志间隔定一定时间后定时发送至指定邮箱

账号及认证管理	支持帐号创建、帐号授权、帐号属性修改、帐号删除等账号管理功能
双机热备	支持双机热备，主备模式、主主负载均衡模式、连接保护模式
	支持两台 WAF 配置同步★
硬件 Bypass 功能	支持开机及断电 bypass 模式，光口支持外置 bypass 模块

5 产品资质

证书名称	**认证机构**
计算机信息系统安全专用产品销售许可证	公安部公共信息网络安全监督局
涉密信息系统产品检测证书	国家保密科技测评中心
计算机软件著作权登记证书	中华人民共和国国家版权局
Web 应用防火墙认证证书	OWASP 互联网安全研究中心
IT 产品信息安全认证证书	中国网络安全审查技术与认证中心
网络关键设备和网络安全专用产品安全认证证书	中国网络安全审查技术与认证中心
IPv6 Ready 产品测试认证	全球 IPV6 测试中心
国家信息安全漏洞库兼容性资质证书	中国信息安全测评中心