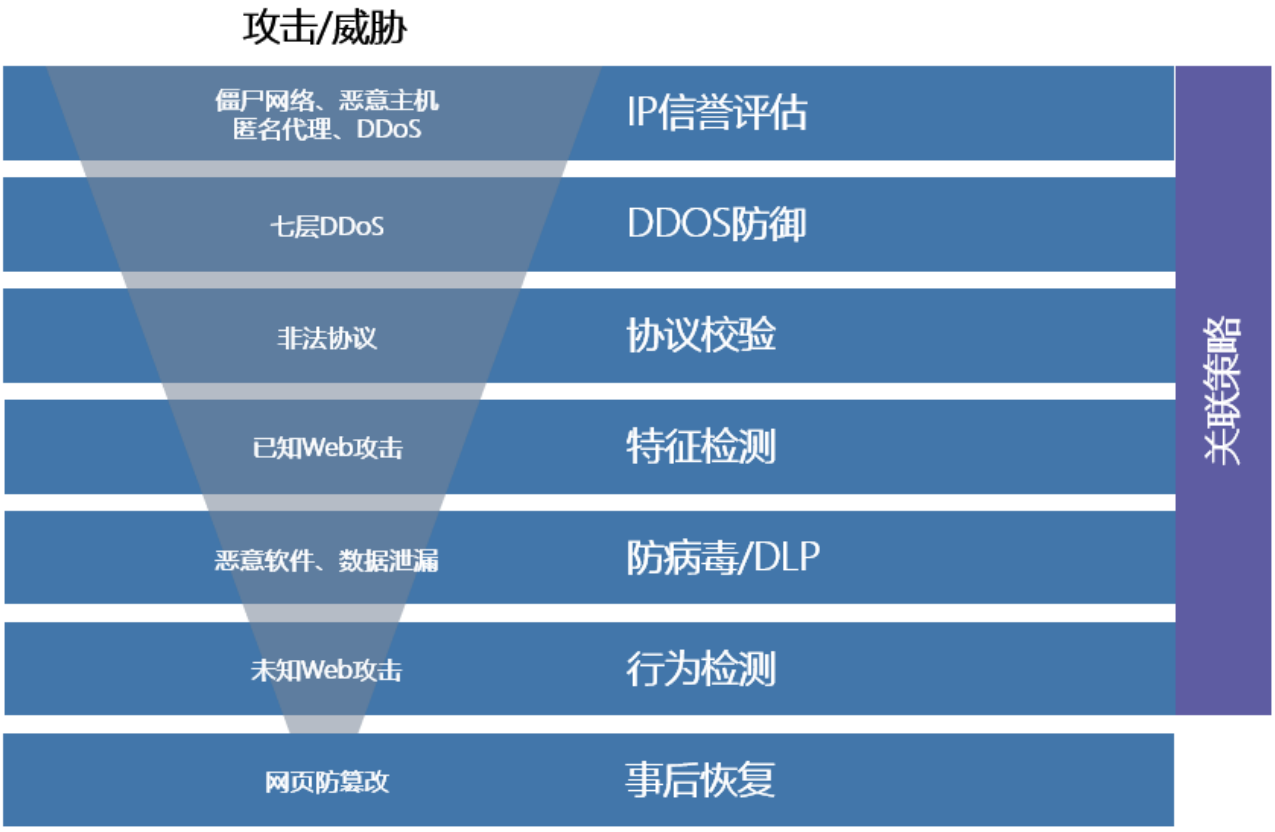
TSINGHUA NOVEL

清华永新 Web 应用防火墙

清华永新 Web 应用防火墙(以下简称清华永新 WAF)为 Web 应用提供高级的多层安全保护 ,包括 OWASP TOP10 及多种已知、未知 Web 安全威胁。

利用清华永新安全云的 IP 信誉服务，清华永新 WAF 能直接自动屏蔽僵尸网络和其它恶意网站。DoS 检测和防御功能让用户的应用始终安全地响应请求服务，而不会被应用层 DDoS 攻击所影响。清华永新 WAF 检查所有 Web 访问请求，通过特征匹配确保访问请求的安全。所有文件、附件或代码都会被清华永新 WAF 自带的防病毒（恶意软件）功能扫描过滤。清华永新 WAF 的自学习检测引擎会复查所有请求，判断是否是攻击行为。如果 Web 请求与用户自定义参数或者机器学习产生的规则不匹配，将被 Web 应用防火墙拦截。

清华永新 WAF 的关联策略引擎将来自多个不同维度的安全事件进行关联分析，确保决策的准确性，同时也可保护 Web 应用不受高级复杂攻击的影响(包括尚未发布特征的 0day 攻击),为 Web 应用提供接近 100% 的安全保护。



产品亮点

防范于未然 – 集成 Web 漏洞扫描

清华永新 WAF 内置 Web 应用漏洞扫描模块，帮助客户以更具性价比的方式满足各类合规要求。清华永新 WAF 的 Web 漏扫可以深入到 Web 应用的组件和元素中，提供深层次的安全隐患检测。Web 漏扫模块定期从清华永新安全云获取更新。

虚拟补丁

清华永新 WAF 通过整合第三方漏洞扫描器（如 AppScan、Acunetix 等），来提供动态的虚拟补丁，为 Web 应用环境提供安全保护。在面对最新 Web 攻击时，第三方扫描器发现的漏洞可以快速自动转化为清华永新 WAF 的安全规则，在开发者修改应用代码之前，提供安全保护。

用户威胁评估与跟踪

Web 应用防火墙的误报会严重影响业务运行。通常情况下，对 Web 应用防火墙策略调优，需要几天甚至数周时间。清华永新 WAF 通过一系列内置工具来解决这个问题，例如告警调整、白名单、自学习、威胁关联检测，以及基于代码的语义分析。

清华永新 WAF 使用用户评分和会话追踪机制，有效降低误报。管理员可以为安全策略添加威胁等级，然后设置触发器的阈值。清华永新 WAF 可以监控用户与 Web 应用间的身份认证，并且监控用户全部行为。所有流量和攻击日志都会与用户名相匹配，以进行用户视角的规则优化和取证。Web 阻挡、告警或监视用户，可以通过归并多个安全事件为用户进行威胁评分，从而提高检测精度，降低误报。

集成应用交付与认证

清华永新 WAF 提供高级的应用层负载均衡与认证卸载服务，支持跨多台服务器进行智能、基于应用的 7 层负载均衡，并在负载均衡时帮助 HTTPS 应用进行 SSL 卸载。使用 HTTP 压缩功能，清华永新 WAF 还可以提升带宽的使用效率，加快响应速度，提高大流量应用的用户体验。

认证卸载可以与多种认证方式整合 ,如 LDAP、NTLM、Kerberos 和 RADIUS ,并支持双因子认证(RADIUS 和 RSA SecurID)。使用清华永新 WAF 的认证服务，用户可以快速发布 Web 站点，并使用单点登录（ SSO ）。快速发布及 SSO 支持多种 Microsoft 应用，如 Outlook Web Access、SharePoint 等。

清华永新 WAF 支持缓存常用 Web 内容，以降低应用的响应时间。当用户向 Web 服务器请求相同资源时，服务器只需响应第一次请求，而之后都由清华永新 WAF 的缓存给予响应，这能够明显提升响应效率，优化用户体验。

虚拟化和云部署

清华永新 WAF 提供高弹性 ,支持用户的虚拟化和云环境。虚拟化版本的清华永新 WAF 的功能与硬件 WAF 完全相同，并且支持全部主流的 Hypervisor 平台，包括 VMware、Microsoft Hyper-V、Citrix XenServer、开源 Xen、KVM 等。清华永新 WAF 支持完善丰富的 RESTful API，帮助用户建设 DevOps 运维体系。

功能特性

部署模式

- 反向代理
- 透明代理
- 完全透明
- 旁路检测
- WCCP

Web 安全策略

- 机器学习（白名单）
- Web 服务与应用特征
- IP 信誉
- 地址信息
- RFC 合法性检测

Web 攻击保护

- OWASP TOP 10
- 跨站攻击
- SQL 注入
- 会话劫持
- 内置 Web 漏扫
- 虚拟补丁
- 支持多条链路防护，数量不限

安全服务

- Web 服务签名
- XML 和 JSON 一致性检查
- 防恶意软件
- 协议检查
- 防暴力破解
- 防 Cookie 投毒
- 错误信息与代码保护
- OS 入侵检测
- 0day 攻击检测
- DoS 防御
- 多事件关联分析
- 防数据泄漏
- 防网页篡改
- 客户端 IP 黑白名单控制
- 触发安全规则阻断告警
- 重定向 URL
- 攻击者 IP 黑名单阻断
-

应用交付

- L7 服务器负载均衡
- URL 重写
- 内容重写
- HTTPS/SSL 卸载
- HTTP 压缩
- 缓存

认证

- LDAP/Radius 认证
- 站点发布
- 单点登录（SSO）
- 双因子认证
- SSL 客户端认证

管理

- Web 管理 & 命令行
- RESTful API
- 日志与报表提供按小时、日期、月份生成
- 实时监控仪表盘
- SNMP/Syslog/邮件告警/手机短信
- 能详细记录攻击事件 HTTP 请求头信息，含请求的 URL、UserAgent、POST 内容，cookie 等所有的请求头内容
- 记录服务器响应头信息，服务器响应内容
- 审计正常访问流量记录、查询所所有用户对网站的访问情况
- 分析访问量最大的 URL、IP 地址、文件

其它

- IPv6 支持
- HA（多设备配置同步）
- 硬件 Bypass
- 自动创建配置
- 配置向导
- 支持 OpenStack
- 支持 WebSocket

关于清华永新

成都清华永新网络科技有限公司，依托清华大学国家重点实验室网络行为研究所数十年累积的雄厚技术力量和科研技术成果，专注于网络信息安全，运用人工智能等前沿 IT 技术运用，为政府、企业、金融、运营商等客户提供覆盖特征安全、行为安全、数据安全的整体安全解决方案。

公司主要研发队伍来自于安全领域的资深专家，包括多位曾任职于 Juniper、Fortinet、Cisco 等国际领导安全厂商核心

研发团队的海归人士。公司致力于将中国顶尖学府多年积累的优秀科研成果与国际先进安全技术结合，积极推动我国自主知识产权下的具有国际领先技术的下一代网络安全平台的应用，积极推进高度可信的，适应中国网络空间需求的智能化安全解决方案。

产品参数表

指标	TN-SG5000-WEB-1000E
吞吐量	1.3Gbps
延时	亚毫秒级
高可用性	A-A、A-P
应用许可	无限制
管理域	64
硬盘	≥4TB
部署模式	支持虚拟化支持 KVM、Xen、VMWare 等虚拟机环境，并支持 WAF 镜像导入
接口	2x GE SFP+
	4x GE SFP
	8x GE RJ45（4 bypass）
电源	100–240V AC，50–60Hz，标配冗余热插拔电源
外观	2U
尺寸（H × W × L，mm）	89× 437 × 456
重量	12.8KG
工作温度	0-40℃
工作湿度	10-90%，不凝露
最大功率	140W