工程成果	WEB 应用安全云服务系统
申请人	马多贺
团队成员	宋晨 杨婧 黄亮 吕双双 李乃山 陈凯 胡建康 马多贺
申请人自述	（请简述工程成果的目的和意义，解决了什么问题，有何贡献或影响，在何处应用，应用效果等。总字数不超过 1000 字，可附页） “WEB 应用安全云服务系统”是在中科院先导专项子课题“海云信息安全体系研究”和国家发改委信息安全专项“基于云的应用安全防护服务产业化”的支持下，针对日益严峻的 WEB 安全形势以及传统硬件网关难于扩展等问题，构建的一套弹性 WEB 应用安全云服务平台。 该系统基于云计算技术，可实现按需定制防护虚拟机，灵活拓展防护能力，为 WEB 应用提供弹性、易管理、一体化的安全保障服务。系统能够有效解决以下三方面的问题，其一，将应用防护能力“虚拟化”，解决了传统硬件网关因受其硬件、软件资源的限制，在防御能力、响应速度等方面无法随需求进行弹性伸缩的问题；其二，将系统维护工作“统一化”，解决了传统硬件网关由于分散部署所带来的在管理、升级以及维护方面的问题；其三，将应用安全水平“全局化”，解决了传统硬件网关因受地域、网络部署环境限制，无法协同为同一区域、同一行业的整体安全水平的评估提供有效支撑的问题。 “WEB 应用安全云服务系统”由实时防护与安全监测两大功能组成,一方面能够对海量 HTTP 数据流进行实时过滤,有效拦截 WEB 攻击，抵御应用层 DDoS 攻击，另一方面集成了篡改检测、挂马检测、关键字与漏洞扫描功能，能够快速感知网页动态，有效识别恶意内容，从而为 WEB 应用提供全方位安全保护。 其主要创新贡献包括以下几个方面： 1、设计了一种分布式弹性防护体系架构，可根据服务规模自适应调节系统容量，实现海量资源按需分配、动态调度，全面保

障系统高可用性与高可靠性；

2、提出了一种网页挂马检测技术，采用“爬虫加代理”的深度探测模式，能够准确挖掘隐藏在网页深处的恶意链接，实现网页挂马行为的快速感知；

3、突破了一种恶意 WEBSHELL 检测方法，基于决策树学习模型克服了传统特征匹配方法的不足,能够准确检测变异 WEBSHELL，同时结合 BOOSTING 方法可进一步提升检测能力；

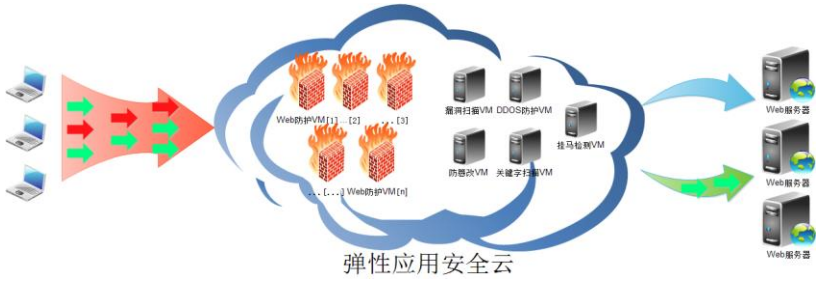

图 1 WEB 应用安全云服务拓扑

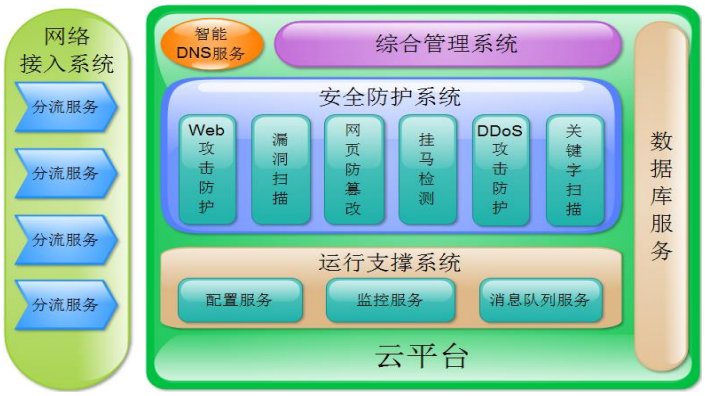

图 2 WEB 应用安全云服务系统架构

本系统重点针对众多分散的 WEB 应用系统，解决 WEB 应用系统中存在安全问题，通过搭建可辐射地区乃至全国的“WEB 应用安全防护云”，为区域以及行业的 WEB 应用系统提供高保障水准、低使用成本、易于接入和管理的应用安全防护服务。

作为“海云”子课题 2012 年率先落地的工程项目之一，本系统十一月份已经完成一期研发，进入试验验证阶段，主要应用效果包括：

1、成功完成深圳高交会展示，该展示对应用安全云服务理念以及技术的推广起到了重要的作用，起到了良好的示范效应；

	2、作为海云创新试验环境的内容组成，在实验室机房已部署一套演示系统，可对外提供WEB应用安全防护服务； 3、与中科院网络中心合作，搭建“海云”项目应用安全云服务的试点应用，现已完成前期准备，开始进入具体实施阶段。