工程成果	基于 SDN 的弹性应用安全云服务平台
申请人	马多贺
团队成员	宋晨、杨婧、黄亮、李乃山、陈凯、吕双双、汤伟、王淼、郭川
申请人自述	“基于 SDN 的弹性应用安全云服务平台”研发出了包括“WEB 攻击防护”、“DDoS 防护”、“挂马检测”、“敏感信息过滤处置”等多种网络安全虚拟化功能。平台采用云计算和 SDN(软件定义网络)技术，充分利用了 SDN 将控制转发分离的新型网络架构，实现安全功能按需定制，为 WEB 应用提供弹性、易管理、全方位的安全保障，有效解决了以下问题： 1) 将安全防护“精细化”，解决了传统防护系统无法按需定制防护类型和防护能力的问题,能够对不同的 WEB 应用提供更细致更有针对性的防护方案。 2) 将安全维护“集中化”，解决了传统防护系统由于地理位置松散无法进行统一维护升级的问题,能够节省大量的人力物力成本的同时控制维护风险。 3) 将安全水平“同步化”，解决了传统防护系统防御水平依赖于管理者知识水平的问题,能够及时将单个 WEB 应用系统出现问题的解决方案同步到所有使用云服务的 WEB 应用系统中，以保证安全云服务防护水平的一致性。 “基于 SDN 的弹性应用安全云服务平台” 由安全防护与异常分析两大功能组成，安全防护能够对主流的 WEB 攻击、DDoS 攻击等进行拦截、防御；异常分析能够通过分析数据流生成正向行为模型，从而阻断异常访问行为。主要的创新贡献包括以下几个方面： 1、提出一种基于 NFSV（网络安全虚拟化）和 SDN（软件定义网络）的安全功能按需定制方案，实现了 SQL 注入、XSS 跨站脚本、DDoS 攻击过滤、蜜罐牵引等攻击防护功能的动态组合和弹性虚拟扩展；采用高速调度和数据并发分析技术，通过自动配置 SDN 控制器策略对数据流向进行定向牵引，从而实现并行化的安全检测

	与防御，简化云环境中安全检测硬件的部署方式，实现低延迟、高性能的安全检测与防御系统； 2、首次定义了针对 SDN 控制器的“盲 DDoS”攻击，研究了基于控制器资源池的防御方法，在此基础上控制器收集盲 DDoS 攻击特征形成防御策略，通过下发防御策略到 SDN 交换机以完成对盲 DDoS 攻击的拦截,解决了单控制器容易成为盲 DDoS 攻击弱点的问题； 3、设计了一种基于网络全局拓扑关联和异常行为的对等 BotNet 检测架构。该架构采用云服务平台的分布式网络交换机作为数据采集探针，利用了 SDN 集中控制、分散采集的特点，有效解决了 P2P 僵死网络难以检测的问题。 “基于 SDN 的弹性应用安全云服务平台”已经完成二期研发，作为“海云”先导专项子课题的先行示范项目，已进入试点应用阶段，取得的应用效果包括： ➢ 中国科技网示范应用 部署了面向科学院各分散的科研 WEB 系统提供统一应用安全保护的云服务平台，目前平台运行良好，有效抵御了包括 Struts2“0day”漏洞利用等高危攻击。 ➢ 新疆“天山云”示范应用 在重点区域电子政务系统上成功部署 WEB 防护系统，拦截了百余次攻击，为进一步接入安全云服务平台构建基础。 ➢ 国家“863”规划课题“SDN 规模验证与应用示范” 推进基于 SDN 的统一安全，面向未来 IDC 数据中心和试点应用。 ➢ “北京云基地”安全云服务试点应用 目前已经完成前期准备，进入具体实施阶段。