面向网站应用的 SDS 自适应安全防御体系

卢梦瑶，唐洪玉，唐维，张鉴
（中国电信股份有限公司研究院云安全工程研究中心，北京 102209）

摘　要：自适应安全架构依托持续性监测与回溯分析形成了集防御、监测、响应、预测为一体的安全防护体系，对于高级定向攻击具备智能与弹性安全防护能力。通过对自适应安全及软件定义安全框架进行研究，结合现有网络安全现状，对网站应用安全问题进行分析，并提出了一种可实现的自适应安全防护平台的初步应用。

关键词：自适应安全框架；云安全；软件定义安全；网站应用安全
中图分类号：TP309
文献标识码：A
doi: 10.11959/j.issn.1000−0801.2020315

Adaptive security architecture defense platform based on software defined security

LU Mengyao, TANG Hongyu, TANG Wei, ZHANG Jian
Institute of Cloud Security, Research Institute of China Telecom Co., Ltd., Beijing 102209, China

Abstract: Based on continuous monitoring and retrospective analysis, adaptive security architecture was constructed to be security defense system integrating prevention, detection, response and prediction, which possesses intelligent and elastic defense ability concerning about advanced directive attacks. An essential implementable adaptive security defense platform was therefore introduced and applied correspondingly according to a thorough research of adaptive security architecture and software defined security, combined with internet security environment. Besides, website application security issues were also analyzed.

Key words: adaptive security architecture, cloud security, software defined security, website application security

1　引言

随着互联网承载的内容和形式越来越丰富，其所面临的安全威胁也越来越多。在互联网经济发展的浪潮中，云计算时代的开启，使得网络环境更加开放、复杂，网络边界愈发模糊[1]，攻击目标也逐步从公共互联网向工业互联网转移，国家网络空间安全受到更深层次挑战[2]。攻击者可利用安全薄弱设备对其他链路设备发起安全攻击，以其为跳板将木马病毒、蠕虫病毒或其他（如拒绝服务攻击等）恶意威胁通过内部流量快速感染至其他主机。与此同时，安全策略不统一、管理环境复杂同样是一项巨大挑战，在物理机/虚拟机、私有云/公有云共存时，复杂的云环境无法满

收稿日期：2020−10−13；修回日期：2020−12−04

足安全管理策略和安全防护能力的协同统一。除此之外，安全产品自身属性也随之发生变化，目前多数安全产品基于政策并受合规驱动，而非来源于用户的实际需求，市场整体趋于碎片化。传统的安全设备以硬件为主，具有部署繁复、功能重叠、无法处理多层流量和数据、无法灵活编排等劣势。但从安全的本质来看，安全是敏捷的、持续发展的，随着黑客攻击和威胁数量的增加以及安全设备与智能终端更加开放泛化[3]，针对关键信息基础设施的高级威胁持续增加，安全威胁变得更加具有针对性、技术含量也更高，目前而言高级定向攻击已经能绕过传统防火墙和黑白名单的预防机制进行定向攻击。

由此可见，随着网络边界模糊、安全硬件固化、安全终端泛连接的特点日益显著，应急响应的安全服务模式已经不能满足未来对于新型攻击和未知威胁的需要。在这种严峻的网络安全形势下，企业对高水平网络安全的需求日益增加，传统安全体系框架在面对新的威胁和攻击显得已经力不从心，在此背景下，具有较为明显优势的自适应安全架构（adaptive security architecture，ASA）应运而出，以应对上述诸多问题。

2 自适应安全与 SDS 软件定义安全概述

ASA 是 Gartner 于 2014 年提出的面向下一代的安全体系框架，以应对万物互联时代所面临的高危攻击频发的安全形势，自适应安全框架的发展经历了 1.0、2.0、3.0 的更新与蜕变[4]。

美国国家标准与技术研究院（National Institute of Standards and Technology, NIST）在 2014 年发布了 1.0 的网络安全整体架构，分为三大组件，核心层、实施层和实例化层。核心层的整体结构与自适应安全架构的 3 个领域概念互相重合，分别是保护、检测和响应，同时在实施的第四层设置为“自适应”层。由于自适应安全架构受到了网络安全整体架构的影响，因而 2014 年到 2016 年可以定义为自适应安全架构 1.0 时期[5] 。2017 年自适应安全架构发展进入了 2.0 时期，主要是在 1.0 的基础上进行了相关的理论丰富，自适应架构 2.0 如图 1 所示[4]。与自适应架构 1.0 相比，自适应架构 2.0 的主要变化包括持续的可视化和评估及 UEBA 相关的内容；在 4 个维度形成闭环之外，形成各自小循环体系以表示各维度所承担的角色功能；在大循环以政策和合规为准线，对框架进行约束。 此架构的提出，主要针对的是高级攻击而形成的高级防御架构，同时将策略与

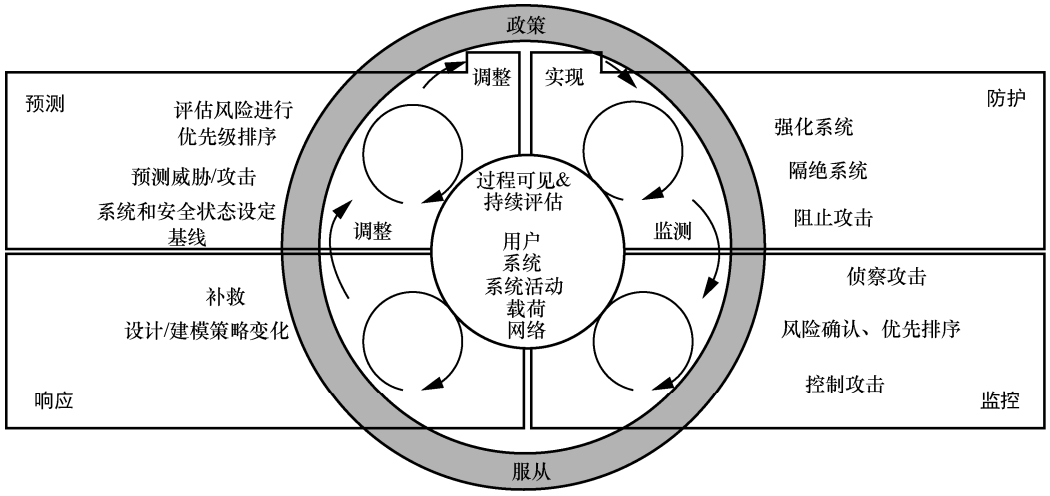

图 1 自适应架构 2.0

合规问题吸纳进来，将自适应安全架构的外延整体扩大，增强了此架构的普适性。

自适应架构 3.0 如图 2 所示[5]，与之前相比，最大的变化是增加了访问闭环，同时将云访问安全代理（CASB）自适应的架构作为原型迁移到了总体架构中。发展到自适应架构 3.0 阶段，自适应安全架构已具备了防御、检测、响应、预测四大基本能力，用于评估攻击行为特征、降低信息系统的威胁攻击面和影响，并通过智能分析和溯源预判，动态精准预测未知攻击，从而构成整个自适应安全防御体系的闭环[6]。

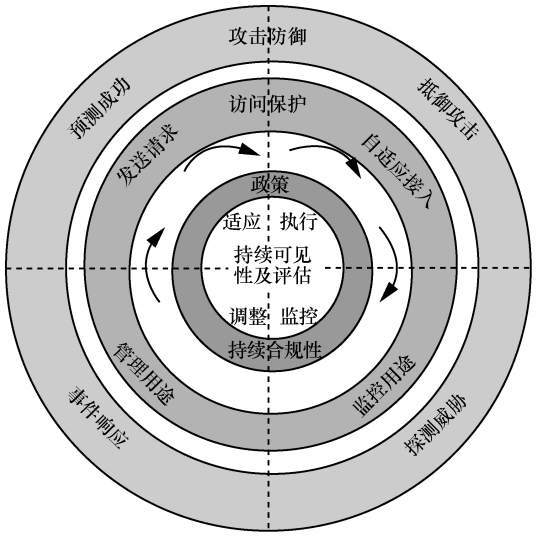

图 2　自适应安全 3.0 框架[5]

软件定义安全（software defined security，SDS）由软件定义网络（software defined networking，SDN）引申而来，将物理及虚拟的网络安全设备与其接入模式、部署方式、实现功能进行了解耦，底层抽象为安全资源池里的资源，顶层统一通过软件编程的方式进行智能化、自动化的业务编排和管理，以完成相应的安全功能，从而实现一种灵活的安全防护。SDS 架构通过将安全功能进行切割形成虚拟化网元，由安全平台统一管理与调度、按需灵活组网，对外提供安全服务，实现资源利用最大化，具有轻量级、易部署、高兼容的优势，能够提供可编排的定制化服务[7]。

3　网站安全中的 SDS 自适应安全防御体系应用

3.1　网站应用目前面临的安全问题

随着互联网承载的内容和形式越来越丰富，网络环境中安全威胁也越来越多，保证网络连接的可靠性、安全性，成为保障网站应用安全的重中之重。面临日益碎片化的安全市场与持续增加的蠕虫、DDoS 攻击以及高级持续定向攻击等各类网络威胁，自适应安全防护框架逐步进入大众的视野。当前网站应用面临的问题，主要包括 XSS 跨站攻击、SQL 注入、网络钓鱼、恶意代码、RootKit 隐身技术、网络端口扫描，针对应用层漏洞的攻击、内网安全威胁等。委内瑞拉大规模停电、俄罗斯 50 多家大型企业遭受未知攻击者勒索、万豪国际酒店 5 亿多条数据泄露等安全事件的发生，无不暴露了当前网络环境中随处可见的安全风险，随着相关网络安全犯罪呈现出新的变化和趋势，数据安全、网站安全面临着前所未有的威胁。

究其原因，除了网络协议本身的缺陷和漏洞之外，可从系统本身和管理策略两个维度进行分析[8]。由于操作系统和应用系统体系结构复杂，硬件工艺或性能缺陷、软件模块接口和系统设计与实现等开发环节的疏忽，都会给网站安全留下巨大隐患，导致网络中断、系统崩溃、数据丢失等结果；另外一方面，由于安全管理人员水平参差不齐，访问控制等主要安全策略设计不当，安全管理制度体系不健全，配套监督机制缺失等，会同样对网站应用安全造成潜在威胁。因此，为了减少威胁攻击响应滞后时间、对安全威胁进行实时阻断、提高网络性能，需要构建动态响应的自适应安全防御体系模型，以此形成系统的自我管理闭环，提升网络系统运行的可控性和抵御攻击能力，保证信息传递的安全可靠。

3.2 SDS 自适应安全防御体系应用

本文提出一种基于 SDS 的自适应安全服务框架，并基于该框架设计了服务平台——安全帮®，作为该框架实践应用的尝试，安全帮®自适应安全云框架如图 3 所示。其可通过结合大数据分析、AI 技术自动完成自适应安全防御模型匹配与业务编排，实时生成自动化响应策略并集中调度安全资源进行能力关联与自动化执行，供覆盖多业务场景的自动化、智能化安全协同防护能力，逐步形成“安全大脑”的全闭环安全智能协同体系。

由图 3 可以看出，基于软件定义安全（SDS）的自适应安全框架不仅融合了软件定义安全的轻量级、高兼容、易部署、可编排的特性，还同时具备了自适应安全框架持续监测和访问控制的特有优势，同时可根据访问的上下文和访问行为进行综合研判，动态变更权限等。与依托被动的纵深防御相比，此框架的提出，可实现主动防御与持续响应，形成具备自适应、威胁情境感知、动态调整的智能防御体系，面对不可避免的安全风险时，具备主动防御与弹性部署的防控能力，为企业创造一个可信任的网络环境，真正解决云安全威胁。

基于 SDS 的自适应安全服务平台，在中国电信安全帮®平台得以研发实现。安全帮®是中国电信研究院云安全研究所自主研发的智能 SaaS（software as a service，软件即服务）安全服务平台，具备即开即用、按需订购、深度跟踪、在线集约运营等服务能力，实现多层面全自助式的安全服务 SaaS 化交付，支持安全业务的自适应智能决策，应对复杂场景的精细化安全服务能力交付、业务灵活定义与协同响应，并对外提供多种标准化产品/服务。

安全帮®自适应安全架构实践如图 4 所示，以软件定义安全架构为基本骨架，结合大数据分析与人工智能技术，形成满足高并发、高可用、分布式部署的需求自适应安全云架构设计；形成安全资源池技术标准，并遵循云安全基础能力体系构建安全资源池；自主开发自适应安全云，形成

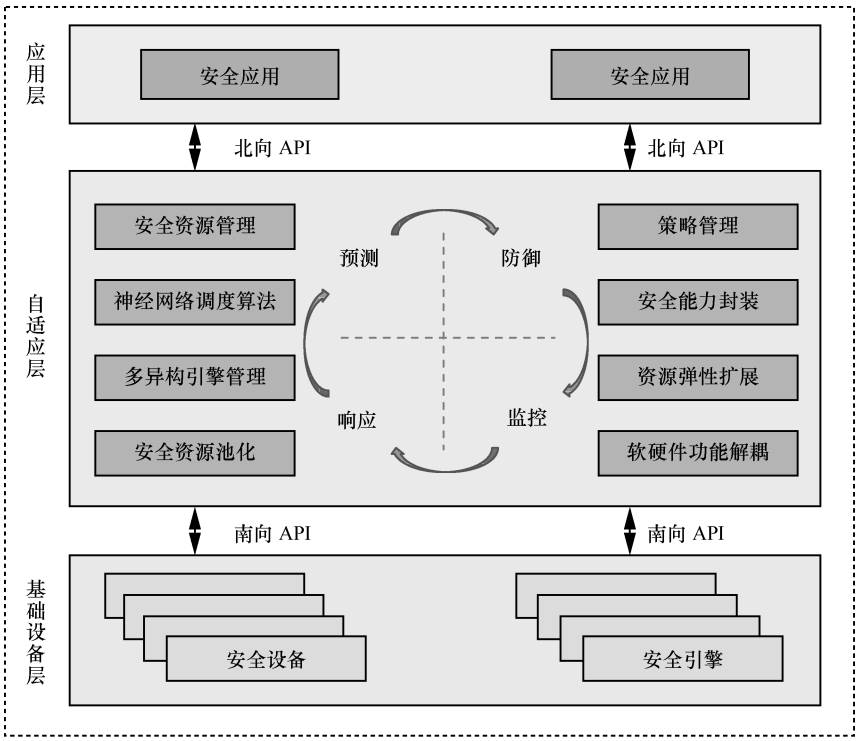

图 3 安全帮®自适应安全云框架

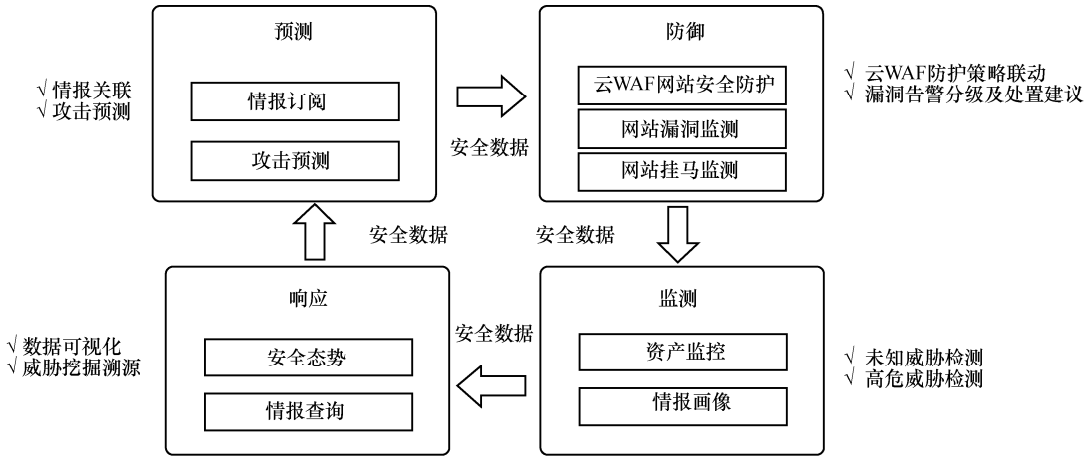

图 4　安全帮®自适应安全架构实践

安全资源集中管理与调度能力，支持安全业务自定义编排与自动化执行，与自适应安全模型配合形成持续处理的、循环的实时动态分析过程；基于失陷场景构建自适应安全防御模型，区别于依赖多维度安全能力叠加的传统防御模式，强调基于业务自内而外构建闭环安全体系，使安全防护变成一项持续响应、处理和优化的过程；进行自适应安全防御模型的安全服务能力规划与填充，结合机器学习，构建多种安全机制间智能联动，定义自动决策算法；实现混合安全资源池中多厂商异构安全资源统一管理与高效的自动化调度，支持安全手段的实时弹性响应与策略的动态高效调整与执行。

与传统的安全防御体系架构相比，安全帮®自适应安全架构通过将主动防御与弹性部署相结合，主动响应与被动防御相补充的方式，建立协同统一的闭环安全体系，面对新型持续性攻击时，能够通过软硬件解耦、策略管理、安全能力封装等实现防护能力的提升。与此同时，安全帮®自适应安全架构利用神经网络算法，基于字段特征值，对收集的安全设备数据特征信息进行建模提取，对于多事件之间的告警信息进行上下文联动分析。通过利用神经网络算法进行计算信息相似度，并针对单一特定场景对特定攻击的特征向量进行分类，形成防御模型，并利用策略管理对某一攻击行为匹配相应的最优防御策略，提高了防御决策精准度；对攻击行为采取动态防御策略与响应，并根据防御结果将系统中新学习的策略对状态特征库进行更新与迭代，整体上做到各环节联动，在自适应安全闭环上实现防护的自动化、灵活化、精准化，具有应急响应性强、可兼容易扩展等显著优势。

综上所述，本文设计并开发的面向网站应用的 SDS 自适应安全架构，将底层安全体系打通，实现安全功能的虚拟化、能力化、智能化、协同化，并通过 SaaS 化的方式交付，从而快速生成契合业务场景的防护体系，形成企业安全的可持续、敏捷、智能、联动的安全防护解决方案。

4　结束语

本文基于自适应安全架构及软件定义安全架构，设计了一种面向网站应用的 SDS 自适应安全平台架构，使得自适应安全架构、云服务平台及云访问安全代理得以有机结合，实现了网站应用安全防护的智能联动闭环。只有深入理解并合理应用自适应安全框架（ASA）框架，才能更有效地构建网络安全新防御体系，提升信息系统安全主动防御能力，最终达到系统安全的可调可控、可视可管、可调度和可持续。

参考文献：

[1] 天融信科技集团. 自适应安全-构建可持续性的威胁防御体系[EB]. 2019.
Tian Rong Xin Technology Co., Ltd. Adaptive security-continuous threat defense system construction[EB]. 2019.

[2] 王伟忠, 张欣, 王大江, 等. 大数据和云计算环境下网络安全分析与解决方案研究[J]. 信息安全与通信保密, 2020(11): 102-110.
WANG W Z, ZHANG X, WANG D J, et al. A research on network security situation and solutions in big data and cloud computing environment[J]. Information Safety and Telecommunication Security, 2020(11): 102-110.

[3] 郑袁平, 贺嘉, 陈珍文, 等. 大数据时代网络安全问题及对策研究[J]. 网络安全技术与应用, 2020(6): 83-85.
ZHENG Y P, HE J, CHEN Z W, et al. A research on network security and problemsin big data era[J]. Network Security and Application, 2020(6): 83-85.

[4] 自适应安全框架（ASA）在网络安全 2. 0 新防御体系中的应用[EB]. 2018.
A new application of adaptive security architecture in network security 2. 0 defense system[EB]. 2018.

[5] 自适应安全架构的历史和演进[EB]. 2019.
Evolution process on adaptive security architecture [EB]. 2019.

[6] 党引弟, 宋宁宁. 动态自适应演进安全架构研究[J]. 信息技术与网络安全, 2019, 38 (10): 18-23.
DANG Y D, SONG N N. Research on dynamic adaptive security architecture with evolution[J]. Information Technology and Network Security, 2019, 38 (10): 18-23.

[7] 陶云祥, 李宙洲. 基于自适应的软件定义安全架构[J]. 电信工程技术与标准化, 2019, 32(6): 66-70.
TAO Y X, LI Y Z. Adaptive software-defined security architecture[J]. Telecommunication Engineering and Standarlization, 2019, 32(6): 66-70.

[8] 李云鹏. 网络安全威胁及防御策略分析[J]. 科技风, 2011(8): 67.
LI Y P. An analysis on network security threat and defense strategy [J]. Ke Ji Feng, 2011(8): 67.

[作者简介]

卢梦瑶（1992− ），女，现就职于中国电信股份有限公司研究院安全工程研究中心运营支撑部，主要研究方向为软件定义安全、云安全。

唐洪玉（1977− ），男，中国电信股份有限公司研究院安全工程研究中心运营支撑部主任，主要研究方向为云安全、威胁检测、态势感知。

唐维（1981− ），女，现就职于中国电信股份有限公司研究院安全工程研究中心运营支撑部，主要研究方向为软件定义安全、云安全、威胁情报。

张鉴（1976− ），男，中国电信股份有限公司研究院安全工程研究中心运营支撑部高级工程师，主要研究方向为云安全、安全攻防、5G 安全。