拟态防御技术在云数据中心的成套部署应用研究

许 辉 郭 兵 马 刚 程怀哲 张 波
河南省信息咨询设计研究有限公司 河南 郑州 450008

摘 要：拟态防御技术以动态异构冗余架构为基础，通过动态或负反馈控制机制控制执行体的更替、上下线、清洗等操作，为此攻击者需付出极大的攻击成本和攻击代价，从根本上满足信息系统具备自我免疫、主动防御的需求。通过对理论背景、特点和发展现状的分析，结合已建设或正在建设的经验，研究提出在云数据中心场景下的拟态防御技术部署方案，并探讨了拟态防御部署发展和挑战。

关键词：拟态防御技术；云数据中心；部署；发展和挑战

1 前言

随着信息技术的快速发展，网络攻击手段日益多样化和复杂化，传统的安全防护措施（如防火墙、入侵检测系统等），大多采用静态防御策略，即基于已知漏洞和攻击模式预设防御规则。然而，这种机制对于未知攻击或零日漏洞的防护能力有限，已难以应对日益增长的安全威胁。为了更有效地应对未知威胁和减少对人工干预的依赖，需要一种能够主动适应威胁变化、自我进化的防御技术。

针对传统安全技术不能从根本上解决未知威胁的难题，邬江兴院士自主原创的拟态防御技术（CMD）[1]，我们称之为“未来网络安全发展的中国新范式”，拟态防御技术应运而生，并逐步进行推广应用。

2 拟态防御的技术背景、特点及优势

2.1 传统安全防护的局限

随着数字化社会的飞速发展，网络空间安全面临着前所未有的挑战。传统的网络安全防护手段主要依赖于边界防御和附加式防护措施，如防火墙、入侵检测系统等。这些手段虽然在一定程度上提高了网络系统的安全性，但存在以下局限性。

无法应对未知威胁：传统防护手段主要基于已知攻击特征进行防御，对于未知威胁往往束手无策。

单点故障风险：许多防护措施部署在单一节点上，一旦该节点被攻破，整个系统可能面临瘫痪风险。

附加式防护引入新风险：在引入新的安全功能时，也可能带来新的内生安全隐患。

2.2 拟态防御技术理论的特点及优势

邬江兴院士受自然界中的拟态现象启发，于2008年首次提出并创建了网络空间拟态防御理论。经过十多年的研究和开发，拟态防御已经具备了大规模产业化的基础。

DHR[2]技术相对传统安全具有显著的结构优势，内生安全机制属于系统先天性的非特异性免疫机制，能够针对各种网络威胁和安全攻击形成普遍防御能力；当前主流的安全机制属于外挂式的后天性的特异性免疫机制，主要对确定性威胁行为或攻击采取防护措施。内生安全机制可以融合当前或未来的防御技术和安全手段，构建集先天性免疫与后天性免疫为一体的融合式防御体系，既能精确抑制特征行为清晰的网络攻击，也能有效管控未知形态的不确定安全威胁，指数量级提升安全增益。

表1 拟态防御技术与传统安全对比分析

对比内容	传统安全	拟态安全
技术对比	基于于已知知识和特征信息，如病毒库、漏洞库等。通过加密、认证、防火墙等安全措施来保护系统和数据的安全	通过动态异构冗余构造（DHR）和策略性的时空变化，对攻击者呈现出“测不准”的场景，扰乱攻击链的构造和生效过程。
效果对比	主要应对已知漏洞和威胁，相对固定和静态，需要不断更新和升级安全措施。	能够应对未知漏洞、后门、病毒或木马等未知威胁。不依赖于先验知识，能够自我不断调整和更新，以适应不断变化的攻击环境。
成本对比	相对较低，主要依赖于现有的安全设备和软件。但由于需要不断更新和升级安全措施，因此成本会逐渐增加	由于需要构建动态异构冗余构造（DHR），因此成本相对较高。但由于能够减少因安全漏洞导致的损失，因此具有潜在的经济效益
场景对比	更适合于对安全性和可靠性要求相对较低的领域，通常可以接受一定的安全风险	更适合于对安全性和可靠性要求较高的领域，如交通、电力、能源、国防等。这些领域通常需要面对复杂多变的网络威胁环境，且对系统的稳定性和安全性有极高的要求

续表：

对比内容	传统安全	拟态安全
部署对比	技术成熟、运维人员众多，有成熟的场景化部署指导文件，技术难题和挑战小	拟态防御技术涉及动态异构冗余架构（DHR）、拟态伪装策略、多维动态重构机制等多个复杂的技术环节。这些技术的实现需要专业的技术人员进行深入的研究和开发，同时也需要运维人员具备较高的技术水平和维护能力。技术复杂度高可能导致部署和维护过程中遇到更多的技术难题和挑战

拟态防御技术是由输入代理、异构执行体、负反馈控制器，以及执行体池和动态调度组成。

与现有安全技术相比，拟态防御技术融合了多种主动防御要素，包括动态性、异构性、冗余性、多模裁决机制等，其主要特点包括：

2.2.1 动态性。拟态防御技术采用功能相等，结构异构的异构执行体池组成，动态调度、管理异构执行体池内各执行体的上线、下线以及清洗、恢复。使得系统对外呈现动态可变的特征。

2.2.2 异构性。异构执行体池中存储了具有功能等价的异构执行体，异构执行体根据工作状态分为工作集和非工作集。

2.2.3 冗余性。拟态防御技术基于冗余性异构执行体，冗余执行体数量可为奇数位（3、5、7等），冗余执行体基于裁决策略通过对同一个输入消息的多个响应结果进行裁决，以保证输出数据的安全性。

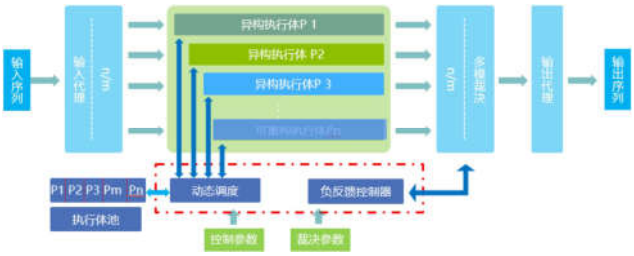

图1 拟态防御技术理论示意图

拟态防御技术部署意义重大，市面上产品包含拟态赋能工具、内生安全网络、拟态安全产品、拟态云计算、拟态应用软件等多款拟态防御产品已在政府、事业单位、军队、电信互联网、公安、金融、企业等多个行业开展了应用试点及示范，取得了显著成效。

3 拟态防御技术部署方案研究

3.1 云数据中心部署方案

云计算中心的安全域一般划分为核心业务域、运维管理域、核心交换域、互联网出口域，根据网络安全等级保护条例要求，拟态防御技术部署需要通过建设“一张安全的网”和“一朵安全的云”分别对通信网络、区域边界、计算环境进行管理，实施多层隔离和保护措施，构建网络安全纵深防御体系。

3.2 新建数据中心部署方案

目前针对新建云数据服务中心，按照云数据中心业务种类、防护重点及安全策略不同，将云数据中心从整体上划分业务区、安全运维区、业务出口区、网络安全区4个安全技术区域：

3.2.1 业务区即安全计算环境。采用拟态防火墙，对云服务环境进行策略管控及安全防护；对于加密型WebShell、变形payload、及0day等攻击的防御则由拟态web防御系统来完成；

3.2.2 安全运维区。采用拟态防火墙对总出口进行策略管控及安全防护；采用拟态安全交换机，定位网络威胁和异常，针对拟态产品与传统安全产品高度兼容的特点，使用传统日志审计、运维平台、漏洞扫描、终端管理系统、数据库审计、终端威胁防御系统对整个系统设备进行统一监控、日志收集、审计、漏洞扫描、备份管理、远程维护等安全运维管理；

3.2.3 业务出口区。采用拟态防火墙对总出口进行策略管控及安全防护；采用传统安全产品检测进出网络内部的数据，对数据进行病毒扫描，检测流经的数据流量，对恶意报文进行丢弃以阻断攻击，对滥用报文进行限流以保护网络带宽资源；以及对整个云数据中心用户控制和管理对互联网或其他网络的使用；

3.2.4 安全通信网络。采用拟态路由器和拟态核心交换机实现可信数据交换、路由转发，合理划分安全域，采用拟态VPN，实现基于SSL和IPSEC的安全通信。

3.3 改造数据中心部署方案

针对已投入使用的云数据中心，依托拟态防御技术和网络安全等级保护2.0相关标准，在分析云数据中心安全需求的基础上，开展内生安全云系统架构和关键技术改造，构建云数据中心可信、可控、可管的安全防护体系。

3.3.1 业务服务区即安全计算环境。采用拟态防火墙更换或冗余部署，对云服务环境进行策略管控及安全防护；对于加密型WebShell、变形payload、及0day等攻击的防御则由拟态web防御系统更换或冗余部署来完成；

3.3.2 安全运维管理区。采用内生安全态势感知平台改造，实时分析处理拟态设备的运行状态，深度检测恶

意访问、恶意文件、漏洞利用、信息泄露、WEB攻击、暴力破解、远程控制、APT攻击等网络安全威胁事件，及时发现已知的、未知的安全威胁；

3.3.3 业务出口区。采用部署拟态综合安全网关，简化组网结构，提供路由、NAT、防火墙、链路负载均衡、流量控制、上网行为管理、入侵防御等功能一体化部署。对总出口进行策略管控及安全防护，对数据进行病毒扫描，对恶意报文进行丢弃以阻断攻击，对滥用报文进行限流以保护网络带宽资源，控制用户和管理对互联网或其他网络的使用；

3.3.4 安全通信网络。关键节点采用拟态路由器和拟态核心交换机替换实现数据交换、路由转发，实现网络具备自我免疫、主动防御的内生安全能力。

3.4 方案对比分析

表2 方案对比分析表

对比内容	对比内容			
	方案1：传统安全	方案2：传统+拟态安全	方案3：拟态安全	优劣对比
组网方式	传统安全产品为基础，针对管理域、业务域、交换域、出口域提供分类安全防护	传统安全产品为基础，关键区域增加拟态安全产品，针对管理域、业务域、交换域、出口域提供分类安全防护	以拟态安全产品为基础，针对管理域、业务域、交换域、出口域提供分类安全防护	方案2相比方案1、3组网相对复杂，方案1设备组网成熟，方案3应用案例较少
投资规模	根据企业预算，投资规模可控适中	投资规模较高	投资规模高	方案2相比方案1、3投资规模略微增加，方案3较方案1投资增加较多
升级扩容	升级扩容管理较为简单，	升级扩容管理相对复杂	升级扩容管理复杂	方案2相比方案1、3升级扩容难度适中，方案3较方案1升级扩容复杂
稳定及安全性	满足等保要求，市场资源丰富，但需定期更新和补丁管理，但对未知攻击或零日漏洞的防护能力有限，潜在网络安全风险	根据企业业务发展需要，提供关键区域防范未知攻击或零日漏洞能力，网络安全可控	提供全方位防范未知攻击或零日漏洞能力，网络安全高度可控	方案2相比方案1、3稳定及安全性可控，方案1稳定及安全性较低，方案3网络安全高度可控，适合于对网络安全要求较高的军队、电力等成本不敏感行业

4 拟态防御部署发展和挑战

面向复杂多样的云数据中心应用场景，拟态防御部署在云数据中心，可预见的挑战主要如下：

4.1 技术复杂性与实现难度

拟态防御技术基于动态异构冗余架构，需要对云数据中心的底层硬件、操作系统、虚拟化层、应用层等多个层面进行异构化设计，在保持系统安全性的同时，还需要确保云数据中心的高性能和资源高效利用。如何在异构冗余架构下实现资源的智能调度和优化，是一个亟待解决的问题。

4.2 云计算虚拟机和容器的安全性

随着云计算技术的发展，虚拟机和容器成为了云数据中心的重要组成部分。拟态防御部署需要提供有效的解决方案如虚拟机逃逸、容器间的隔离问题等。

4.3 人才队伍的培养

拟态防御技术的实施需要具备相关专业知识和技能的人才。然而，目前这方面的人才还比较匮乏。因此，需要加强人才培养工作，提高实施、运维、技术支持人员的专业技能和素质。

云数据中心拟态防御技术的部署，基于内生安全理论，通过持续的技术创新、标准化与规范化、云边协同与一体化和智能化运维等多种举措的推进，最终必将形成可持续健康发展的安全技术与产业生态环境。

5 结语

研究拟态防御技术的创新演进和发展对于推动科技进步、促进经济发展以及满足社会安全需求具有重要意义，更是我国十四五重点研发项目。通过深入探讨拟态防御技术的战略发展和实施路径，可以为我国乃至全球的网络安全转型提供有力支持和指导。与现有的基于叠加的附加式防护措施对比，拟态防御技术是一种我国自主原创的全新网络安全体系架构，有利于重构网络安全世界格局，扩大网络安全空间话语权。

参考文献

[1]邬江兴.《内生安全赋能网络弹性工程》ISBN:978-7-03-074585-9[J]科学出版社,2023.7

[2]邬江兴.《网络空间拟态防御原理》ISBN:978-7-03-059096-1[J]科学出版社,2018.11