doi:10.11920/xnmdzk.2025.04.011

基于集约化管理的智能云网安全系统构建与研究

张　波[1],曾　迪[2],蒋　鸣[1],徐　庆[1],仲亚男[1],丁晓嵩[1],陈彦如[2]
(1.中国电信股份有限公司四川分公司,四川 成都 610031;2.四川大学计算机学院,四川 成都 610065)

摘　要:针对当前网络安全防护体系在效率和资源管理方面的不足,提出了一种集约化管理策略,旨在优化网络安全资源的配置与管理.研究分析了智能云网安全防护系统的架构,重点探讨了网络流量控制和安全能力组件的集成方法.结合下一代防火墙、入侵检测系统和 Web 应用防护系统的多维度安全策略部署,阐明了集约化管理在提升安全防护效果中的具体应用.通过对实际案例的实验分析,结果表明,采用集约化管理策略后,系统在长时间流量测试中未出现丢包,单个网元故障切换时业务中断时间仅为 7 秒,两台网元同时故障时流量能够自动绕过,业务中断时间缩短至 15 秒以内,显著提升了网络的稳定性与业务连续性,同时实现了资源的高效利用.

关键词:网络安全;集约化管理;智能云网
中图分类号:TP393.09　　**文献标志码**:A　　**文章编号**:2095-4271(2025)04-0437-09

Construction and research of intelligent cloud network security system based on intensive management

ZHANG Bo[1], ZENG Di[2], JIANG Ming[1], XU Qing[1], ZHONG Yanan[1], DING Xiaosong[1], CHEN Yanru[2]
(1.Sichuan Branch of China Telecom Co., LTD, Chengdu 610031, China;
2.School of Computer Science, Sichuan University, Chengdu 610065, China)

Abstract: To address the inefficiencies and resource management limitations in current network security protection systems, an intensive management strategy was proposed to optimize the allocation and administration of network security resources. The architecture of an intelligent cloud-network security protection system was analyzed, with a focus on the integration methods for network traffic control and security capability components. A multidimensional security policy deployment approach was explored, incorporating next-generation firewalls, intrusion detection systems, and web application protection systems. Practical applications of intensive management in enhancing security protection effectiveness were detailed. Experimental analysis based on real-world scenarios revealed that, with the adoption of the intensive management strategy, the system showed no packet loss during extended traffic tests. In cases of single network element failure, service interruption was limited to 7 seconds, while simultaneous failures of two network elements resulted in automatic traffic rerouting and service interruptions reduced to less than 15 seconds. These results highlighted significant improvement in network stability, business continuity, and resource efficiency.

Keywords: network security; intensive management; intelligent cloud network

在数字化转型的浪潮中,网络信息技术已成为推动工业、金融、医疗等行业创新的关键力量.然而,伴随技术进步而来的网络安全问题愈发严峻,从个人隐私泄露到国家级网络攻击,均凸显出网络安全在保障

收稿日期:2024-11-06
通信作者:陈彦如(1993-),女,副研究员,博士,研究方向:工控安全、区块链、数据智能、工业互联网、物联网.E-mail:chenyanru@scu.edu.cn
基金项目:国家自然科学基金(62302324)

社会稳定与国家安全中的关键作用[1].当前,全球范围内加强网络安全防护已形成共识,各国政府和国际组织通过法规如欧盟的GDPR(通用数据保护条例)等,力求提升数据保护水平,减少安全风险[2-3].

近年来,网络安全研究不断深化,聚焦于威胁识别、分析与防御策略等方向[4-5].传统的安全防御措施在应对日益复杂和动态变化的网络安全威胁时已显现出局限性.集约化管理作为一种新兴管理模式,因其在资源整合与快速响应方面的潜力而备受关注.Kure等人的研究指出,集约化管理通过集中协调与资源整合,有效提升了网络安全威胁的响应速度[6],而Alahmari等人则进一步证明了其在成本效益方面的优势,尤其适用于中小企业[7].然而,目前在智能云网架构下对集约化管理理念的具体应用与技术实现研究仍较为缺乏,特别是在网络安全防护体系的设计上.

将基于智能云网的设计原则,结合集约化管理理念,提出一种新的网络安全防护架构.Yu等人的分层解耦设计原则为集约化管理提供了技术支持[8],而Zhang等人的研究则进一步强化了网络流量控制机制在智能云网安全防护中的关键作用[9].本研究旨在探讨如何将集约化管理理念转化为可操作的技术架构与运营策略,以应对智能云网环境下日益复杂的安全威胁.

本文的主要工作包括以下三个方面:

①提出一种基于智能云网的集约化管理网络安全防护系统架构,设计并创新性地引入了一种全新的软件定义为网络(SDN)流量控制方法,为提升网络安全管理的智能化水平提供了理论支撑.

②构建了一套面向智能云网的安全运营策略,显著增强了网络安全防护的灵活性和整体运行效率,为复杂网络环境下的安全运营提供了实用参考.

③将集约化管理理念应用于电信运营商云计算平台,开展了系统性验证,充分验证了其在资源整合、故障响应和业务连续性保障方面的显著优势,为电信行业的云网融合安全管理提供了实践依据和借鉴意义[10-11].

1 智能云网安全防护系统架构设计

在当今复杂多变的网络环境中,网络安全威胁日益多样化和动态化,传统安全架构逐渐难以满足日益增长的安全需求.智能云网安全防护系统的设计核心在于构建一种兼具灵活性和适应性的架构,以应对当前及未来网络环境中的安全挑战.该架构需具备动态资源分配、高效流量管理以及智能威胁检测的能力,从而在虚拟化和云网融合的背景下,实现对网络流量的精准控制和安全防护.本章将从整体架构出发,探讨其运作机制和技术实现路径,并重点聚焦于网络流量控制机制的设计与优化,以期为智能云网环境下的安全防护提供理论支持和技术框架.

1.1 智能云网安全防护系统的整体架构

云计算和网络融合技术的快速发展使得传统网络安全架构在动态云网环境中面临诸多挑战,如安全策略调整滞后、资源利用效率低、监测能力受限等.这些问题制约了网络安全防护能力的提升,难以满足现代网络对安全性和灵活性的需求.

为此,本研究提出一种基于智能云网的安全防护架构.该架构采用集约化管理与SDN技术,结合分层解耦和流量编排理念,实现安全策略的高效部署与动态调整,优化资源利用效率,并通过服务链编排和负载均衡技术灵活适应网络安全需求的变化.

本研究的核心贡献在于创新性地解决了传统安全架构在云网融合环境下的局限性.接下来,将重点探讨该架构的核心功能之一——网络流量控制机制.该机制通过先进技术手段,实现对网络流量的实时监控、动态管理和精准保护,为智能云网环境下的安全防护提供理论和技术支撑.

1.2 软件定义的网络流量控制:机制、实现与网络安全应用

在网络虚拟化环境中,传统安全架构面临诸多挑战,尤其是虚拟机间流量的监控盲区以及流量管理的静态化,难以应对动态变化的安全威胁.这些问题的核心在于传统安全设备依赖于物理网络路径,无法有效捕获和分析虚拟化环境中的流量,导致安全监控能力受限.此外,传统流量控制方法缺乏灵活性,难以适应虚拟化网络的动态特性,严重制约了网络安全防护能力的提升.

1.2.1 机制和理论基础

为解决上述问题,本研究提出了一种基于软件定义的网络流量控制机制.该机制通过软件定义网络

(SDN)技术,引入镜像技术捕获虚拟化网络中的流量,并利用 SDN 控制器的动态调整能力,实现对流量的实时监控和精准管理.其核心在于打破传统物理设备的限制,通过软件定义接口实现流量的灵活捕获与控制,从而提升虚拟化网络环境中的安全监控能力.

1.2.2　技术实现

在智能云网安全防护系统中,我们面临的主要挑战是如何有效地监控和管理虚拟化环境中动态变化的网络流量.本研究提出的基于软件定义网络(SDN)的流量控制机制,正是为了解决这一问题.该机制通过动态流量捕获、实时分析和全局协调等技术手段,实现了对网络流量的高效监控与灵活管理.

如图 1 所示,镜像网络流量监控与分析流程图展示了这一机制的工作流程.流程从流量的捕获开始,通过镜像流量采集器高效地捕获虚拟化环境中的流量.接着,这些流量被转发至镜像流量分发器,该分发器负责将流量复制并根据预设策略进行分发,以降低业务网络的负载并提升资源利用效率.

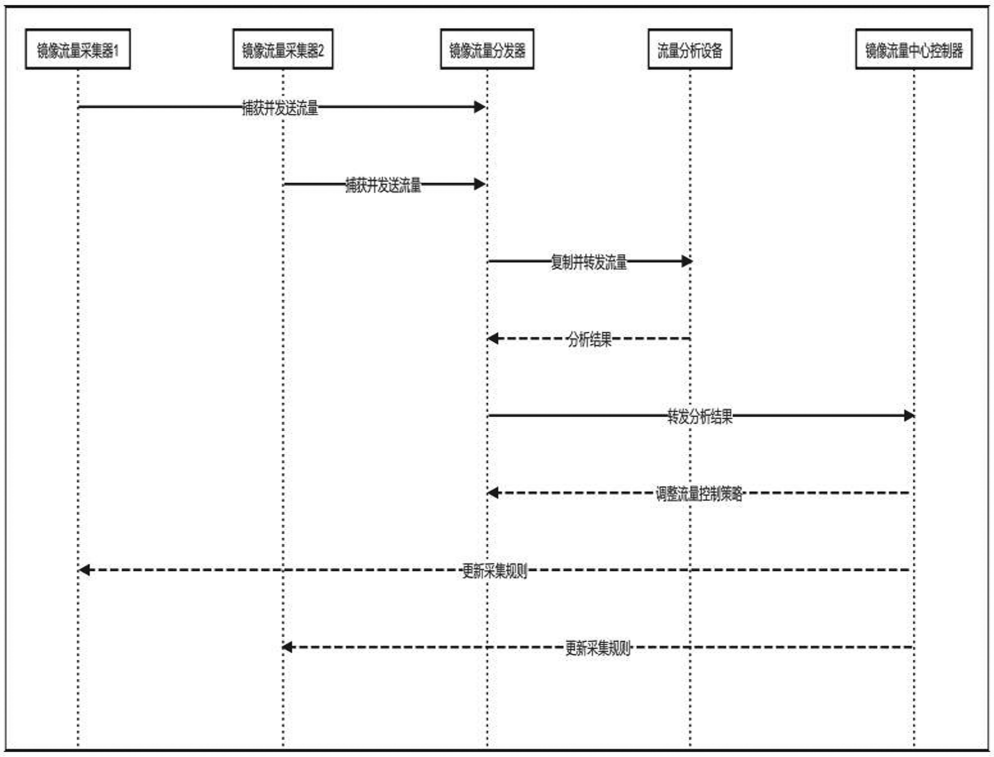

图 1　镜像网络流量监控与分析流程图

Fig.1　Mirror network traffic monitoring and analysis flow chart

随后,流量分析设备接收分发的流量数据,并执行多维度、多层次的流量分析操作.分析结果通过反馈机制回传至流量分发器,为动态策略调整和实时流量管控提供了依据.最后,镜像流量中心控制器作为全局控制模块,统一管理和协调各组件的工作流程,通过提供软件定义的接口,支持灵活调整流量控制策略,并确保组件间的协同与整体系统的高效运转.

通过这一流程,本研究提出的流量控制机制不仅解决了传统方法在虚拟化环境中的局限性,还显著提升了流量监控和管理的精准性,为云网融合环境下的网络安全提供了高效、智能的解决方案.

1.2.3　工作流程

网络流量控制机制的核心挑战在于实现对网络流量的实时监控、动态管理和精准保护.本研究提出的工作流程通过一系列紧密衔接的步骤,解决了传统方法在虚拟化环境中的局限性,显著提升了流量管理的效率和安全性.

该流程开始于数据包的捕获,其中镜像流量采集节点实时捕获虚拟化网络中的数据包,并在本地流表中进行规则匹配.如果匹配成功,则执行相应的转发或过滤操作;如果没有匹配规则,则向中心控制器发起规则请求.这一过程确保了流量管理的准确性和连

续性.

当中心控制器接收到规则请求后,它基于流量特征进行分析,并检索或动态生成新规则.新生成的规则迅速下发至采集节点,以实现数据流的快速转发与精准管控.捕获的流量随后经由镜像流量分发器进行复制与分发,根据预设的流量控制策略,将流量高效分配至多个流量分析设备.

分析设备对流量进行深入处理,包括异常行为检测、协议分析等,并将分析结果反馈至中心控制器,用于进一步优化系统策略.系统通过对未知流量模式的智能分析,持续提升流量控制策略的精确性.此外,各节点基于实时流量特征动态更新流表,以优化资源利用率并避免重复捕获.系统还支持实时删除冗余规则,进一步提高流量管理的效率和稳定性.

图2展示了整个流程的详细步骤,包括数据包的捕获、规则的生成与下发、流量的分发以及动态更新等环节.整个流程由中心控制器作为智慧中枢进行统一协调,确保各环节的高效协作.通过软件定义的接口,中心控制器显著提升了系统策略调整的灵活性,并增强了其在动态网络环境中的适应性.

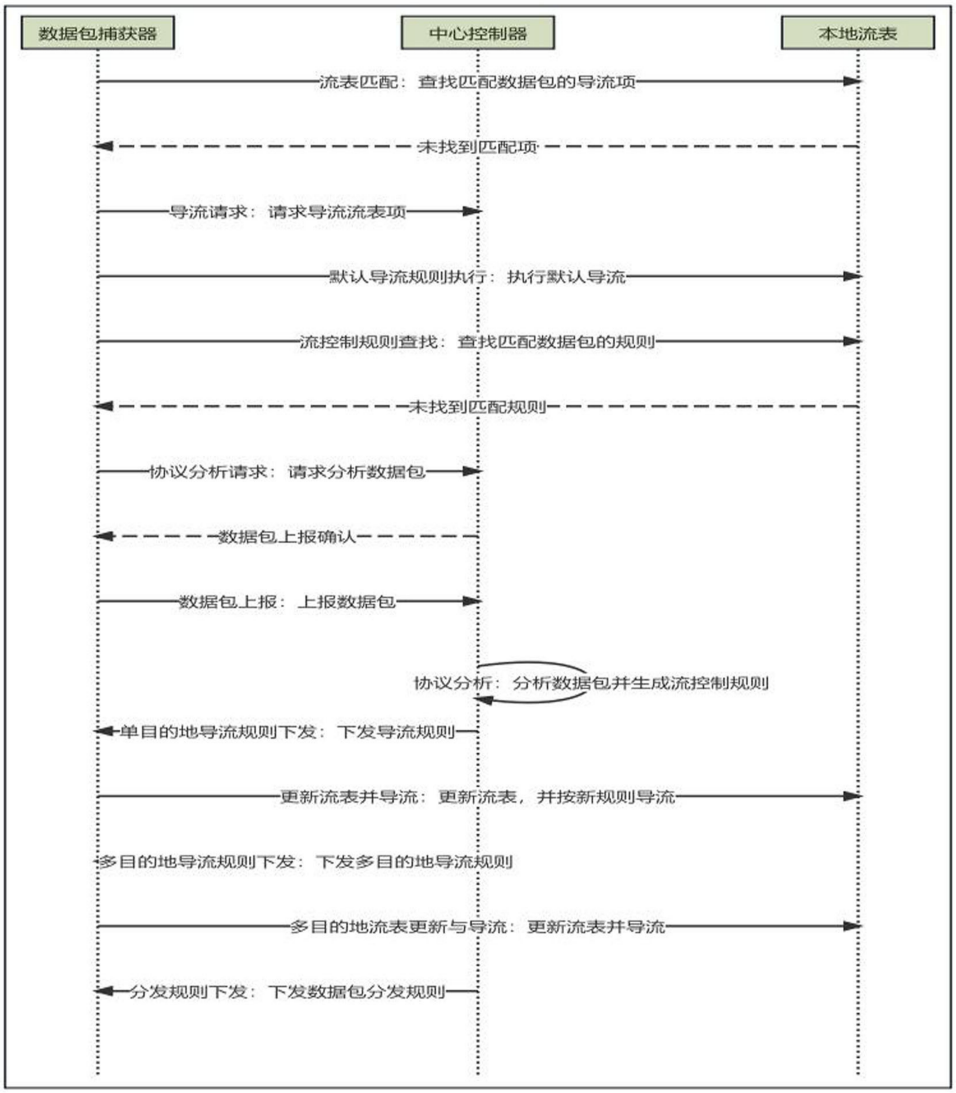

图2 镜像流量管理详细流程图

Fig.2 Detailed flow chart of mirror traffic management

这一闭环工作流程使网络流量控制机制能够高效、精准地监控和管理虚拟化网络中的流量,同时快速响应潜在威胁,为虚拟化网络环境中的安全防护提供了一种可行且高效的解决方案.

1.3　综合安全能力集成:构建智能云网多层次防护体系

在前文对网络流量控制机制的探讨中,我们认识到,尽管基于软件定义的方法能够显著提升网络安全需求响应的效率与智能化水平,但单一的流量控制机制并不足以构建全面且稳固的网络安全防线.因此,本研究进一步探讨了如何通过集成多种安全能力组件,实现多层次的防护体系与综合化的安全管理策略,以应对复杂多变的网络威胁.

本研究旨在解决的关键问题包括:如何有效地整合不同的安全技术以形成一个协同工作的防护体系,以及如何通过智能化手段提升网络安全管理的整体效能.为此,我们提出了一个智能云网安全防护系统框架,该框架通过集成下一代防火墙(NGFW)、入侵检测系统(IDS)、入侵防御系统(IPS)和 Web 应用防火墙(WAF)等关键安全组件,实现了从网络边界到应用层面的全面保护.

该框架的核心贡献在于其能够通过行为审计、病毒防护、漏洞扫描、网站信息安全监测、舆情监控和智能运维等多种安全能力的协同,增强安全防护的深度和广度.这些安全能力组件不仅提供了传统的安全防护功能,如应用识别、入侵防御、恶意软件拦截等,而且还通过采用大数据和机器学习等先进技术,实现了对网络安全威胁的智能识别和响应.如表 1 所示.

表 1　智能云网安全组件功能概述

Table 1　Overview of intelligent cloud network security components function

安全组件功能	解释
行为审计	上网行为审计,对操作行为识别并审计的过程,分析防护目标服务及流量行为.
病毒防护	在网关处主动过滤拦截病毒、木马、间谍软件等恶意软件,在病毒未进入内部网络造成损失之前进行阻断拦截,有效避免了病毒所给用户带来的损失和影响.
漏洞扫描	漏洞检测扫描服务,提供全面、快速、精准的漏洞扫描及风险监测服务,持续发现暴露在互联网边界上的常见安全风险.
网站信息安全	网站信息安全监测服务,采用大数据构架机器学习算法,准确发现监测网站暗链、挂马、不良信息安全事件.
舆情云	舆情监测以全网数据监测、智能语义分析为技术支撑,全方位整合传统媒体、门户网站、微信、视频、微博、论坛、海外媒体等舆情信息,可实时追踪热门舆情信息.
智能运维	智能运维系统,对主机和应用进行监控,系统性能、组件服务、数据库、日志等等关键性能指标进行监测及预警,统一操作维护、执行作业计划.

此外,本研究还强调了集中管理平台在智能云网安全防护系统中的重要性.集中管理平台通过单一控制台实现所有安全组件的集中配置和管理,简化了管理流程并提高了效率.其实时监控功能和自动化响应机制确保了对安全事件的快速识别和处理,而策略同步功能和标准化接口则促进了不同组件间的无缝集成,提升了系统的兼容性和扩展性.

综上所述,本研究提出的智能云网安全防护系统框架,不仅解决了如何有效整合多种安全能力组件的问题,而且还通过智能化手段提升了网络安全管理的整体效能,为应对不断变化的网络安全环境提供了一种全面且高效的解决方案.

2　集约化网络安全防护系统的应用与验证

在前文中,我们对智能云网安全防护系统的理论基础和架构设计进行了详细分析,确立了集约化管理在提升网络安全防护效率和效果中的核心地位.本章将对我们设计的框架系统进行介绍,并将其应用于电信运营商云计算平台,验证其资源整合与快速相应的优势.

2.1　实施背景与目标

随着信息化进程的加速,网络安全威胁呈现出复杂化和多样化的趋势,传统网络安全架构在应对实时威胁、防止资源浪费以及支持新兴技术方面表现出明显局限性.为了应对这些挑战,提出了一种基于集约化管理的智能云网安全防护系统(MSSP).该系统通过分层解耦设计,使各安全能力模块实现独立管理与动态调整,降低系统复杂度;利用软件定义网络(SDN)技术,实现对安全资源的智能调度与流量路径规划;结合大数据分析和机器学习技术,提升安全威胁的实时感知和响应能力;并通过虚拟化技术提高资源的共享性和利用效率.MSSP 旨在打造一个高效、灵活的网络安全平台,整合智能化资源,实现安全能力

的统一管理和灵活调度,从而提升对复杂网络安全威胁的响应效率与效果.

2.2 MSSP 整体架构

MSSP 的整体架构由地市安全资源池和安全运营管理中心两大核心模块组成,二者协同工作,实现网络安全资源的智能调度与高效利用.

地市安全资源池作为流量接入和处理的中心,利用虚拟化技术(如 KVM)部署网元设备(如 vRouter)引导用户流量,并通过动态加载安全能力模块(如下一代防火墙、入侵防护系统)来根据流量特性分配所需的安全资源.此资源池基于 X86 或 ARM 架构的服务器进行高效汇聚,并支持多租户环境下的隔离与调度.

安全运营管理中心作为 MSSP 的管理中枢,负责统一调度与控制地市资源池和安全能力,核心功能包括跨区域的安全策略管理、资源优化调度和全网安全态势的可视化监控.通过 SDN 控制器,运营管理中心能够动态调度流量,将用户的流量分配到最优的安全资源池,并基于大数据分析平台提供实时威胁预警与响应.该中心采用分布式架构,结合机器学习算法提升威胁感知能力,并通过 API 接口与地市资源池无缝对接.

如图 3 所示,MSSP 整体架构展示了从地市资源池到运营管理中心的协同工作流程,系统通过虚拟化和智能化手段构建了高效、安全、可扩展的网络防护体系.MSSP 架构的优势在于通过资源整合提升资源利用率,避免传统架构中资源分散的弊端.利用 SDN 技术动态分配资源,提升安全防护的灵活性与响应速度,同时架构具备良好的扩展性,能够根据业务需求扩展资源池容量或加载新的安全能力模块,从而满足不同用户的定制化需求.总体而言,MSSP 通过虚拟化与智能化技术构建了一个高效、安全、可扩展的网络防护体系,确保了资源的高效利用与灵活调度.

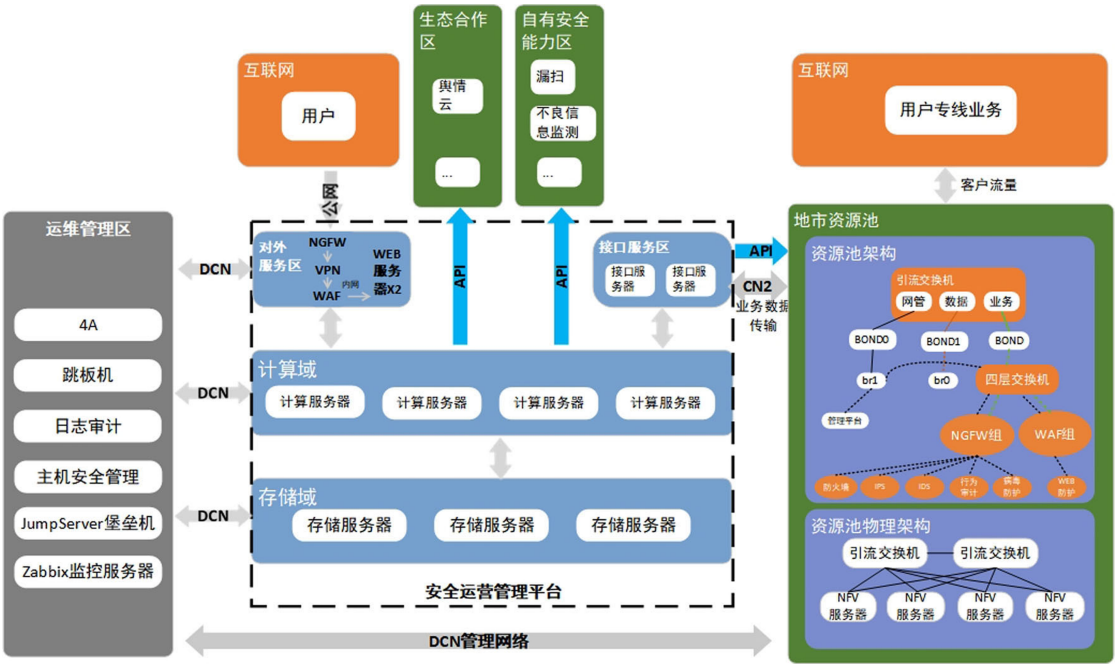

图 3 MSSP 整体架构

Fig.3 MSSP overall architecture

2.3 MSSP 系统方案

2.3.1 设计思路

MSSP 的设计遵循“集约化、多手段、多层次”的原则,旨在构建可持续运营的网络与信息安全服务能力.该系统面向基于千兆光网的互联网专线等典型应用场景,支持实现租户管理、自助服务、统一策略管理以及服务链编排等功能模块,为多样化的安全需求提供灵活支持.

如图 4 所示,安全能力共享平台与安全云资源池集群在城域网数据中心内设计并部署,形成整体架构.当服务实体订购特定的安全能力后,其流量经城域网核心路由器(CR)接入引流隧道,并通过策略路由转发至安全云汇聚交换机.安全管理平台基于软件定义网络(SDN)的流量编排能力,将流量动态引入对

应的安全资源池.资源池内的虚拟化网络功能(NFV)化安全设备负责提供包括流量防护、威胁检测和数据可视化在内的综合性安全服务,从而实现高效的安全资源共享与动态调度.这些功能与 MSSP 功能框架中的各层密切相关,为系统的整体功能实现奠定了基础.

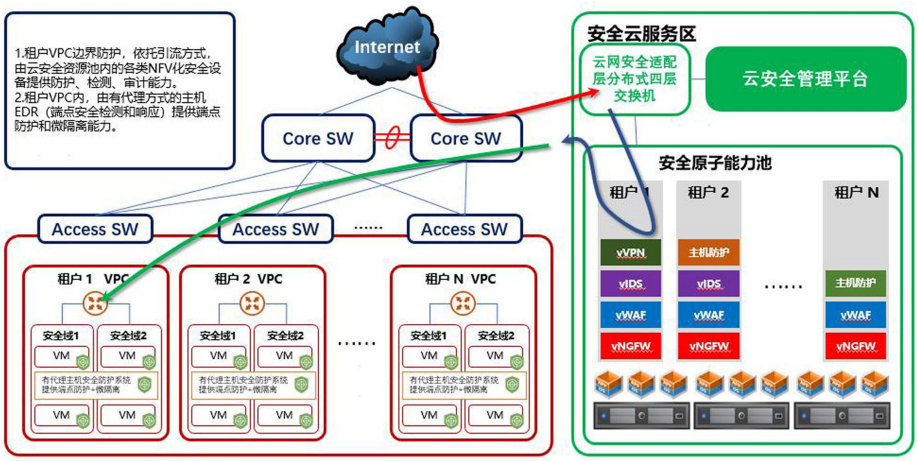

图 4　MSSP 方案

Fig.4　MSSP solution

2.3.2　MSSP 功能框架

如图 5 所示,MSSP 功能框架的设计分为 5 个层次,每一层都承担着独特的职责,共同构建了灵活高效的安全服务体系.

虚拟化层:基于 KVM 虚拟化系统,提供虚拟网元和流量引流功能,确保系统的灵活部署和资源动态分配.

虚拟化安全能力层:集成 NGFW、IPS、WAF 等安全能力,支持虚拟化部署与动态调用,强化系统安全防护.

安全能力适配层:统一管理底层虚拟化能力,支持能力的注册、编排与 API 对接,实现系统与外部的无缝连接.

安全管理平台:集成服务对象、运营和运维需求,提高系统管理效率,涵盖安全态势展示、服务订购和资源池管理.

安全服务能力层:提供全面的安全服务,包括防火墙、入侵防护、漏洞扫描等,构建全面的网络安全防护体系.

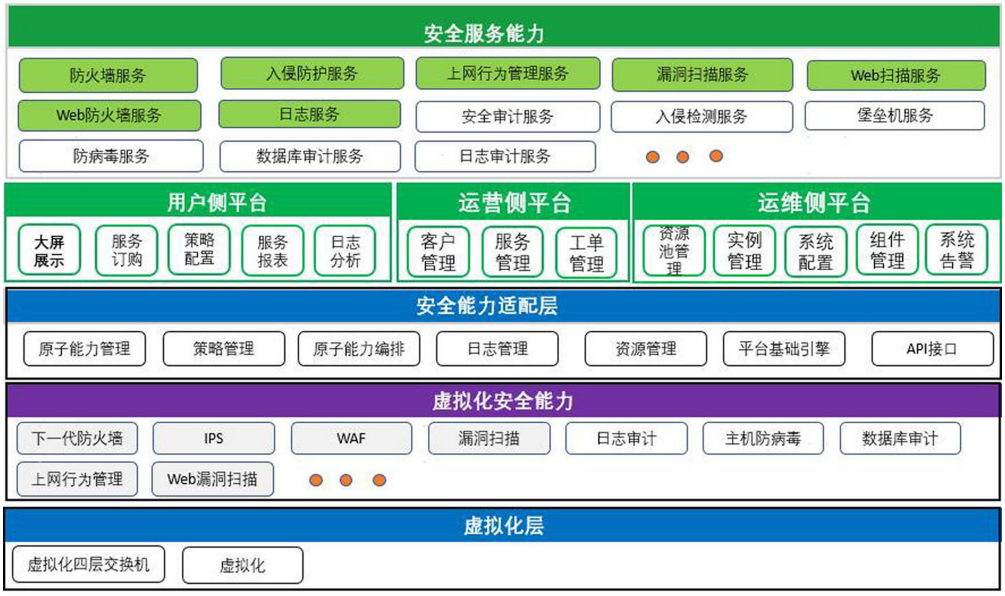

图 5　MSSP 功能架构

Fig.5　MSSP functional architecture

MSSP 通过多层次、虚拟化和智能化的架构设计,确保了资源的高效整合和安全能力的灵活调度.在这一框架中,安全资源的动态调配与高效利用得到了充分体现,同时系统具备了强大的拓展性和可持续性,能够应对不断变化的安全需求.

2.4 MSSP 性能评估与实验结果

本节基于实验结果,从网络性能、可用性和功能完整性三个方面对 MSSP 进行了全面评估,旨在深入分析系统在实际应用中的表现.通过对流量稳定性、时延抖动和丢包率的测试,验证了其在高流量场景下的网络可靠性;通过模拟多种故障场景,评估了系统在网元故障和服务链中断情况下的快速切换与业务连续性保障能力;同时,通过功能测试全面检验了系统对引流配置、安全服务配属以及资源创建与管理的支持水平,综合展示了 MSSP 在智能化调度和资源整合方面的显著优势.

在网络性能测试中,MSSP 表现优异,如表 2 所示,长时间流量测试未出现丢包,且时延抖动稳定在 50 ms 以内,体现了系统的高稳定性.

表 2 网络性能测试结果表

Table 2 Network performance test results

测试项	测试场景	时延抖动(ms)	丢包率(%)
ping 大包测试	靶机引流后	31	0
长时间流量稳定性测试	安全资源池流量引流	49	0

在可用性测试中,模拟多种故障场景,以测试 MSSP 在面对防火墙故障,WAF 故障的情况下,业务中断时间与丢包数量,如图 6 所示,体现了系统能有有效地保障业务连续性.

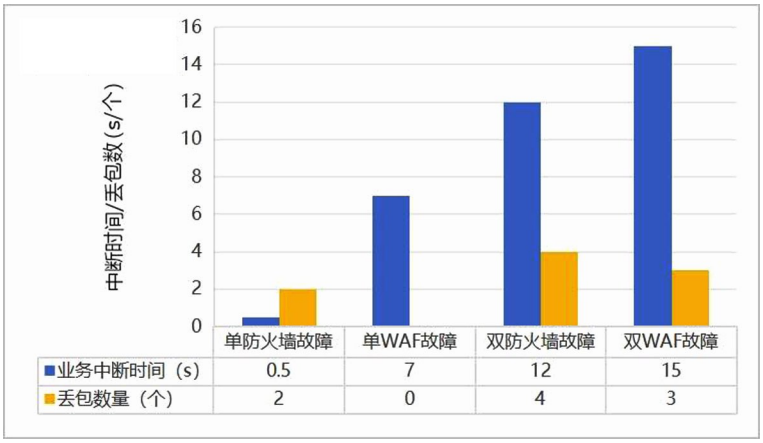

图 6 故障切换测试结果

Fig.6 Failover test results

功能测试中,资源池在引流配置,安全服务管理以及资源创建与删除等操作中表现正常,如表 3 所示,MSSP 始终可以保持功能完善且操作灵活.

表 3 功能测试覆盖表

Table 3 Functional test coverage table

功能测试项	预期结果	实测结果
添加、删除引流配置	功能正常	通过
安全服务配置调整	功能正常	通过
创建与删除网络资源	功能正常	通过
用户创建与删除	功能正常	通过

总体而言,MSSP 通过集约化管理策略和智能化调度技术,显著提升了网络资源的利用效率和安全防护的响应能力,为复杂网络环境中的安全运营提供了强有力的技术支撑和实用参考.这些成果不仅证明了系统的高性能和可靠性,也为进一步优化和推广提供了重要的实践依据.

3 结论

智能云网安全防护系统的发展离不开技术的持续进步.人工智能、机器学习等新兴技术将在提升系统智能化和应对复杂威胁方面发挥重要作用.随着云服务和远程办公的普及,安全解决方案需要不断适应新场景的需求.未来,通过技术创新和灵活的架构设计,安全系统将进一步增强对复杂威胁的响应能力.同时,推动行业合作、优化用户安全意识培训,也将为构建更加稳固的网络安全生态提供支持.通过这些努

力,智能云网安全防护系统将持续优化,以更好地应对复杂的网络安全挑战,保障网络环境的安全与稳定.

参考文献

[1]USSATH M,JAEGER D,CHENG F,et al.Advanced persistent threats:Behind the scenes[C]//2016 Annual Conference on Information Science and Systems(CISS).Princeton:IEEE,2016:181-186.

[2]朱玉明.论国家安全中的网络安全[D].湘潭:湘潭大学,2006.

[3]EU.Regulation(EU)2016/679:General data protection regulation(GDPR)[S].Official Journal of the European Union,2016.

[4]DU D J,ZHU M G,LI X,et al.Areview on cybersecurity analysis,attack detection,and attack defense methods in cyber-physical power systems[J].Journal of Modern Power Systems and Clean Energy,2023,11(3):727-743.

[5]CASCAVILLA G,TAMBURRI D A,VAN DEN HEUVEL W J.Cybercrime threat intelligence:A systematic multi-vocal literature review[J].Computers & Security,2021,105:102258.

[6]KURE H I,ISLAM S,MOURATIDIS H.An integrated cyber security risk management framework and riskpredication for the critical infrastructure protection[J].Neural Computing and Applications,2022,34(18):15241-15271.

[7]ALAHMARI A,DUNCAN B.Cybersecurityrisk management in small and medium-sized enterprises:A systematic review of recent evidence[C]//2020 International Conference on Cyber Situational Awareness,Data Analytics and Assessment(CyberSA).Dublin:IEEE,2020:1-5.

[8]余小军,吴亚飚,张玉清.云安全体系结构设计研究[J].信息网络安全,2020,20(9):62-66.

[9]张国新.5G“云网边端”一体化纵深安全防护体系研究及应用[J].电信科学,2022,38(10):173-179.

[10]张连营,胭騄,黄嘉骏,等.集约化电子政务云技术方案研究[J].电信科学,2022,38(Z2):331-338.

[11]杨经纬,胡林,李金岭,等.支撑电信运营商集约管理的云计算平台研究探索与实践[J].电信科学,2013,29(8):136-145.

[12]KAUR R,GABRIJELČIČ D,KLOBUČAR T.Artificial intelligence for cybersecurity:Literature review and future research directions[J].Information Fusion,2023,97:101804.

[13]THAWAIT N K.Machinelearning in cybersecurity:Applications,challenges and future directions[J].International Journal of Scientific Research in Computer Science,Engineering and Information Technology,2024,10(3):16-27.

[14]YOON C S,HONG C H,KANG M S,et al.Quantum asymmetric key crypto scheme using Grover iteration[J].Scientific Reports,2023,13(1):3810.

[15]SCARANI V,BECHMANN-PASQUINUCCI H,CERT N J,et al.The security of practical quantum key distribution[J].Reviews of Modern Physics,2009,81(3):1301-1350.

[16]佟得天,刘旭东,郭涛峰,等.云计算信息安全分析与实践[J].电信科学,2013,29(2):135-141.

[17]张鉴,唐洪玉,刘文韬,等.面向云网融合的电信网安全防护体系参考架构[J].电信科学,2020,36(5):10-15.

(责任编辑:张阳,殷锋,付强,和力新,肖丽;英文编辑:周序林,郑玉才)