

面向网络安全资源池的智能服务链系统设计与分析

王泽南¹, 李佳浩², 檀朝红³, 皮德常²

(1. 网络通信与安全紫金山实验室, 江苏 南京 211100; 2. 南京航空航天大学, 江苏 南京 211100;
3. 江苏省未来网络创新研究院, 江苏 南京 211100)

摘要: 传统网络安全架构通过将流量引导经过硬件形式的网络安全功能设备来保障网络安全, 该架构由形式固定的硬件组成, 导致网络安全区域部署形式单一, 可扩展性较差, 在面对网络安全事件时无法灵活地做出调整, 难以满足未来网络的安全需求。面向网络安全资源池的智能服务链系统基于软件定义网络与网络功能虚拟化技术, 能够有效解决上述问题。基于网络功能虚拟化技术新增虚拟形式的网络安全功能网元, 结合已有的硬件网元构建虚实结合的网络安全资源池, 并基于软件定义网络技术实现对连接网元的交换设备的灵活控制, 从而构建可动态调节的网络安全服务链; 基于安全日志检测与安全规则专家库实现对网络安全事件的检测与生成对应的响应方案, 从而能够在面对网络安全事件时通过集中式控制的方式实现服务链的动态智能调节; 对服务链的部署过程进行数学建模并设计了一种启发式的服务链优化编排算法, 实现服务链的优化部署。通过搭建原型系统并进行实验, 结果表明, 所设计系统能够在面对安全事件时在秒级时间内完成安全事件的检测, 并能够在分钟级时间内完成对安全服务链的自动调整, 所设计的服务链优化部署算法能够将服务链对虚拟安全资源池中资源的占用降低 65%。所设计系统有望运用于园区与数据中心网络出口处的网络安全区域, 简化该区域的运维并提高该区域的部署灵活度。

关键词: 软件定义网络; 网络安全资源池; 服务链; 网络功能虚拟化

中图分类号: TP393

文献标志码: A

DOI: 10.11959/j.issn.2096-109x.2022051

Design and analysis of intelligent service chain system for network security resource pool

WANG Zenan¹, LI Jiahao², TAN Chaohong³, PI Dechang²

1. Purple Mountain Laboratories, Nanjing 211100, China

2. Nanjing University of Aeronautics and Astronautics, Nanjing 211100, China

3. Jiangsu Future Networks Innovation Institute, Nanjing 211100, China

Abstract: The traditional network security architecture ensures network security by directing traffic through

收稿日期: 2022-05-16; 修回日期: 2022-07-22

通信作者: 王泽南, wangzenan@pmlabs.com.cn

基金项目: 江苏省卓越博士后计划

Foundation Item: Jiangsu Funding Program for Excellent Postdoctoral Talent

引用格式: 王泽南, 李佳浩, 檀朝红, 等. 面向网络安全资源池的智能服务链系统设计与分析[J]. 网络与信息安全学报, 2022, 8(4): 175-181.

Citation Format: WANG Z N, LI J H, TAN C H, et al. Design and analysis of intelligent service chain system for network security resource pool[J]. Chinese Journal of Network and Information Security, 2022, 8(4): 175-181.

hardware based network security function devices. Since the architecture consists of fixed hardware devices, it leads to a single form of network security area deployment and poor scalability. Besides, the architecture cannot be flexibly adjusted when facing network security events, making it difficult to meet the security needs of future networks. The intelligent service chain system for network security resource pool was based on software-defined network and network function virtualization technologies, which can effectively solve the above problems. Network security functions of virtual form were added based on network function virtualization technology, combined with the existing hardware network elements to build a network security resource pool. In addition, the switching equipment connected to the network security elements can be flexibly controlled based on software-defined network technology. Then a dynamically adjustable network security service chain was built. Network security events were detected based on security log detection and a expert library consisting of security rules. This enabled dynamic and intelligent regulation of the service chain by means of centralized control in the face of network security events. The deployment process of the service chain was mathematically modeled and a heuristic algorithm was designed to realize the optimal deployment of the service chain. By building a prototype system and conducting experiments, the results show that the designed system can detect security events in seconds and automatically adjust the security service chain in minutes when facing security events, and the designed heuristic algorithm can reduce the occupation of virtual resources by 65%. The proposed system is expected to be applied to the network security area at the exit of the campus and data center network, simplifying the operation and maintenance of this area and improving the deployment flexibility of this area.

Keywords: software define network, network security resource pool, service chain, network function virtualization

0 引言

随着经济和技术的快速进步,电信业与互联网得到高速发展^[1]。而随着移动互联网时代的到来,网络渗透到了交通、医疗、生产、教育等各个社会层面^[2],网络已经与人们的生活密不可分,随着各种网络技术的发展,网络的安全问题将是未来网络所面临的挑战之一,需要不断地更新、解决与完善。

传统网络安全架构通过将网络数据流量引导经过多个网络安全设备来保障网络通信安全。网络业务发展迅猛,传统网络安全架构面临许多问题,主要体现在如下两方面:首先,网络安全设备多为专用硬件,专用硬件面临造价昂贵、升级困难、部署不够灵活的问题^[3];其次,网络安全设备与网络拓扑结构相耦合,存在扩展性差、管理困难、故障点多、性能受限、安全链路架构单一等问题。

针对上述问题,网络功能虚拟化(NFV, network function virtualization)^[4]技术被提出,NFV旨在利用虚拟化技术把不同的网络功能迁移到标准通用硬件平台上,降低网络硬件成本的同时使网络部署更加灵活可控。软件定义网络(SDN, software defined network)^[5]通过将控制平

面和数据平面分离实现对网络资源的统一灵活控制。NFV和SDN技术两者相互补充。一方面,NFV基于虚拟化技术提供软件形式的网络安全功能,实现网络安全功能的灵活快速调度与部署;另一方面,SDN提供集中式的网络控制能力,实现对网络的整体优化控制决策。两者相互融合可实现按需定制的网络服务^[6]。基于此思路,可以有效地解决传统网络安全架构中存在的上述两个问题。

本文设计了一种面向网络安全资源池的智能服务链系统,该系统基于SDN与NFV技术,支持构建虚实结合的网络安全资源池,支持基于安全日志动态调整安全服务链,以及支持安全服务链的优化部署。虚实结合的网络安全资源池通过在虚拟机中运行虚拟网络安全功能网元,并设计一套安全服务链管理框架,对接虚拟网络与物理交换机,实现网络流量按策略在物理网元和虚拟网元之间按指定顺序流转^[7],从而实现安全服务链的灵活构建与调整。安全服务链的动态调整则通过建立安全规则专家库,对第三方安全网元推送的日志信息进行解析,与安全规则专家库中的触发条件进行匹配,发现安全事件后及时按照预

置规则调整安全服务链。安全服务链的优化部署通过对部署过程进行建模,并调用设计的启发式算法实现服务链的部署,在满足业务需求的同时,最小化所消耗的虚拟资源量。

本文通过搭建原型系统,对所设计智能服务链系统的功能与性能进行验证;通过数值仿真对所提的服务链优化部署算法的性能进行评估,并对实验结果进行分析。实验结果表明,该系统能够实现虚实结合的网络安全资源池的构建,能够面对安全事件时在秒级时间内完成安全事件的检测,能够在分钟级时间内完成对安全服务链的自动化调整,能够将服务链对虚拟安全资源池中资源的占用降低 65%。

1 相关工作

网络安全服务链的主要目标是将满足特定属性的网络流重定向,快速、灵活地牵引网络流经过所需的安全服务节点序列进行安全防护检测,满足用户多样性的安全业务需求。本文基于 SDN/NFV 领域关于安全服务链的相关研究,研究面向网络安全资源池的智能服务链系统。目前与网络安全服务链相关的一些研究工作如下。

Shin 等^[5]提出了 FRESCO 安全架构, FRESCO 安全架构基于 SDN 提出了可重构安全服务模式,其以若干个安全模块组合的方式构建安全服务,如数据包分析、网络流重定向等,利用脚本语言自定义编排这些基本的安全模块,以此生成一条完整的服务链。虽然 FRESCO 将基本的安全模块进行动态的组合,可提供相对复杂的安全功能,验证了安全能力分解和重组的可行性,但其提供的安全服务类型非常有限,仅给出了功能上的验证。

Liu 等^[6]提出了 NFV 架构结合 SDN 构建安全服务链以解决 NFV 架构下的安全性问题,在 NFV 架构中部署软件安全模块并进行合理编排,利用 SDN 控制器的全局拓扑感知与网络流调度能力,依次引导网络流经过特定顺序的软件模块序列进行安全防护检测处理来满足未来网络安全业务需求。

Martini 等^[7]提出基于 OpenFlow 协议构建安全服务链,通过对网络资源进行集中的监控和管理,下发交换机流指令引导网络流到中间设备;基于 OpenFlow 协议的服务质量 (QoS, quality of

service) 字段,对不同网络流的服务需求进行标识,提出了基于服务类型的服务链理论模型,该模型对各种业务 QoS 流进行采集、分析、分类并发送到对应的服务链中进行处理。然而,该方案拓展了 SDN 的南向标准协议,兼容性较差且需预先定义并编排各个服务类型对应的服务链,动态性和灵活性仍存在不足。

Giotis 等^[8]提出了基于策略的网络虚拟资源管理机制,根据策略对用户的安全服务链需求进行描述,网络虚拟资源管理机制通过解析用户策略构建安全服务链,根据用户策略定义的特定网络数据流属性,动态地编排相应的服务节点。该方案具备较好的动态性与灵活性,可依据用户的业务需求灵活地编排安全服务链,但在策略处理方面,并未涉及应用策略更新引起的策略冲突问题。

Qazi 等^[9]提出了在安全服务链中安全资源调度度的研究,为了兼容传统硬件安全设备,在 SDN 中通过手工部署硬件安全设备并配置相应的安全防护策略,进而实现安全防护目标,其主要思想是通过 SDN 的全局拓扑感知与网络流调度能力将业务流重定向并依次引导到网络中预先部署的各种实体安全设备中进行安全防护检测。虽然该方案充分利用了传统硬件安全设备,减少了用户的资源消耗,但该方案拓扑依赖严重、设备之间耦合度较大,且需手工部署安全设备,难以满足用户快速迭代的安全业务需求。

通过对上述研究的梳理不难发现,SDN 和 NFV 技术为解决虚拟化网络环境中的安全防护问题提供了很好的思路,但目前关于如何快速、灵活、智能化地构建安全服务链方面还有待深入研究。如何充分利用 SDN/NFV 技术思想的特点,设计出高效灵活的安全服务链机制,实现自动化的、灵活的、弹性的编排和部署,是现阶段的主要研究方向^[10]。

在此背景下,针对现阶段快速、灵活、智能化地构建安全服务链这一方面的欠缺,本文提出了一种面向网络安全资源池的智能服务链系统,解决传统网络安全服务中设备封闭僵化、网络安全业务部署不灵活,缺乏自适应性等问题,并实现了网络安全服务链的优化编排调度。

2 智能服务链系统设计与实现

2.1 支持网络安全池虚实结合的服务链构建

网络安全资源池主要由硬件形式的网络安全功能网元构成。而在本系统的设计中,参考基于NFV的软件定义安全设计,采用虚拟化的网络安全功能网元。如图1所示,这些网元以独立形态的虚拟化软件形式运行在标准x86服务器上,通过服务器内部的虚拟网络进行通信,构成一个可平滑扩展的网元集群,并通过统一的管控平台实现管控。本系统采用OpenStack平台作为虚拟化平台^[15],为这些虚拟网元提供承载运行的虚拟机载体,并实现相互之间的隔离。

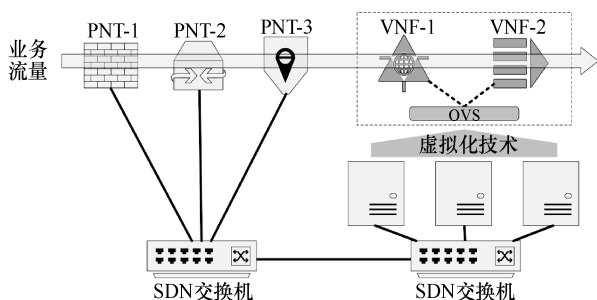


图1 虚实网络功能结合的网络资源池架构设计
Figure 1 Design of network security resource pool architecture combining virtual and physical network functions

本系统将业务流量按照指定顺序转发至不同类型的网元,构成网络安全服务链,服务链中包含物理网络功能(PNF, physical network function)与虚拟网络功能(VNF, virtual network function)^[16]。如图1所示,业务流量经过一条由3个PNF和2个VNF构成的服务链,实现不同网络安全功能的组合。为了实现业务流量按照指定的顺序经过指定类型的网络功能,本系统基于SDN交换机和虚拟网桥构建网络安全功能网元之间的网络连接,并通过SDN控制器实现对SDN交换机和虚拟网桥上转发流表的控制。特别地,在系统实现中,为了加快数据包在VNF之间的转发速度,本系统采用DPDK^[17]技术,加速从服务器网卡到VNF处理进程之间的数据包转发。

2.2 基于安全日志检测的服务链动态更新机制

基于安全日志检测的服务链动态更新机制设计中,主要包括3部分,分别是安全日志解析模块、安全规则库与服务链控制模块。系统通过对

攻击日志的解析得到攻击类型,匹配安全规则库中的安全规则,若找到对应的安全规则,根据规则中定义的规则链动态更新服务链。

具体地,日志解析通过部署SYSLOG SERVER接收第三方安全检测设备推送的日志信息,解析日志信息中属性,包括设备主机名、攻击链、威胁类别、攻击者、威胁严重性、事件可信度等,将这些信息按照预置的攻击事件模板进行整理并生成攻击事件。

安全规则库借鉴专家系统^[18]的设计思路,保存了安全规则配置信息,一条安全规则包括两部分,分别是攻击事件字段与对应的规则链,攻击事件由历史攻击事件组成,而对应的规则链由网络安全专家创建并加入系统中。当日志解析生成攻击事件时,则将该攻击事件与安全规则中的攻击事件字段进行匹配,匹配方式为最长前缀匹配。当匹配成功时,则定位至对应的规则链,并通过服务链控制模块根据规则链中的定义动态更新服务链。

在更新过程中,服务链控制模块首先将规则链与现有服务链对比,如当原有安全网络功能不满足规则链要求、需要添加新的安全功能时,则先删除原有服务链,包括删除物理SDN交换机及虚拟网桥中与该服务链相关的流表信息;然后创建并下发规则链中定义的新的服务链,若新增的安全功能为虚拟网元,则通过虚拟化平台创建新的VNF实例,并配置SDN交换机及虚拟网桥中的流表。

图2展示了服务链动态调整^[19]的使用场景,原始服务链中包含3层防火墙(FW)与Web应用防火墙(WAF, Web application firewall)两个网元。当系统中被注入危险流量时,WAF网元发现该可疑流量并生成日志告警,本系统将接收推送的日志告警并整理生成攻击事件,将该攻击事件与安全规则库中的攻击事件字段进行对比,确定所要调整的规则链,假设规则链告知需要在服务链中增加深度包检测(DPI, deep packet inspection)网元,则服务链控制模块将分配一个DPI网元,该网元可以是PNF,也可以是新建的VNF,随后调整SDN交换机和虚拟网桥上的流表调整转发策略。从上述使用场景示例可见,通过服务链动态更新的机制设置,攻击事件的危险流量流过对应网络安全服务链中的网络安全资源来

进行安全防护，与传统安全网络的串联架构做比较，该机制可以在保障安全性的同时，降低日常网络安全资源池资源开销。

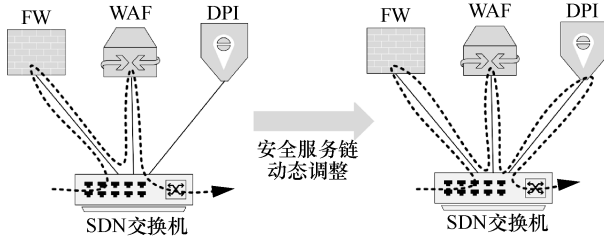


图2 服务链动态调整的场景示例

Figure 2 Example of service chain dynamic tuning scenario

2.3 服务链部署模型与算法

在服务链部署的过程中，需要决定服务链中每个网络功能映射的对象^[20]，以及当映射的对象为 VNF 时决定为该 VNF 分配的资源，保证部署后的服务链满足业务的需求。为了解决这个问题，本节介绍一种服务链部署模型，并针对建立的数学模型提出一种启发式算法。

假设需要部署的服务链包含 I 个网络功能，使用集合 $\{S_1, S_2, \dots, S_I\}$ 表示，其中 S_i 表示第 i 个网络功能。底层网络中存在 J 个 PNF 与 K 个 VNF，分别用集合 $\{P_1, P_2, \dots, P_J\}$ 和 $\{V_1, V_2, \dots, V_K\}$ 表示，其中 P_j 表示第 j 个 PNF， V_k 表示第 k 个 VNF。服务链中的网络功能与底层 PNF 之间的映射关系用 0-1 变量 x_{ij} 表示， $x_{ij} = 1$ 表示 S_i 被部署到 PNF P_j 上，同理， y_{ik} 表示服务链中的网络功能与 VNF 之间的映射关系。由于服务链中的网络功能仅能部署在一个网元上，可以得到 $x_{ij} + y_{ik} = 1$ 。

在本系统设计中，由于任意的 PNF 和 VNF 之间通信最多通过两台 SDN 交换机，可以认为不同网元之间的转发时延近似，将该时延表示为 T_L 。服务链中的端到端时延除了网元间的转发时延，还有数据包经过网元的处理时延，一般认为 PNF 网元的处理时延是固定的，而 VNF 网元的处理时延与为其分配的资源有关。通过实验发现，VNF 对数据包的处理时延与分配的资源基本呈线性关系，如图 3 所示。因此，假设为 V_k 分配的资源为 r_k ，则 V_k 对数据包的处理时延可以表示为 $L_k - \lambda_k r_k$ ，其中 L_k 与 λ_k 的值可以通过实验获得，而 PNF 的转发时延表示为 L_j 。

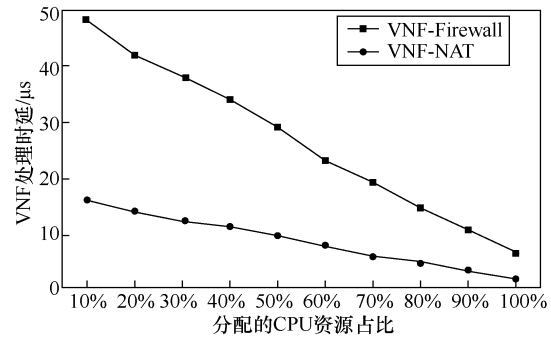


图3 VNF 处理时延与分配资源量的关系

Figure 3 Relationship between VNF processing delay and amount of allocated resource

假设数据包经过服务链的端到端时延要求为 T_D ，则服务链的部署问题可以抽象为确定 x_{ij} 、 y_{ik} 以及 r_k 的值，且保证服务链的端到端时延在 T_D 范围内，即保证式(1)中所示约束成立。本系统设计中，优化目标为最小化网络安全资源池中虚拟资源的占用，因此该模型的优化目标如式(2)所示。

$$\sum_{i=1}^I \left(\sum_{j=1}^J x_{ij} L_j + \sum_{k=1}^K y_{ik} (L_k - \lambda_k r_k) \right) + T_L (I-1) \leq T_D \quad (1)$$

$$\min \left(\sum_{i=1}^I \sum_{k=1}^K y_{ik} r_k \right) \quad (2)$$

为了解决上述模型问题，本文提出一种启发式算法。该算法的核心思路是将服务链中的网络功能优先部署于 PNF，当 PNF 集合中不包含所需要的网络功能类型或所需的 PNF 处理能力不足时，则选择再新建 VNF。当全部网络功能的部署映射对象确定后，推导计算数据包经过 VNF 所被允许的最大时延，由式(1)可知该时延等于 T_D 减去数据包经过 PNF 的时延与网元间转发时延累计值，然后将这些 VNF 按照 λ_k 的值从大到小进行排序，依照排序结果依次为 VNF 分配所允许的最大资源量，直至服务链的端到端时延满足业务要求。

3 实验与分析

3.1 实验环境搭建

本文所设计的原型系统中硬件包含 4 台服务器，2 台 SDN 交换机，1 台 3 层防火墙设备，以及 1 台 WAF 设备。服务器配置为 24 核 CPU，频率为 2.1 GHz，内存 64 GB。其中 3 台服务器安装运行 OpenStack J 版本，为 VNF 提供基础虚拟机

环境, 1 台服务器用于运行 SDN 控制器。SDN 交换机采用盛科 V580, 3 层防火墙设备采用华为 USG6300, WAF 设备采用深信服 B1400。硬件设备之间的连接参考如图 1 所示方式进行。

对于本文所提的服务链编排映射模型与算法, 采用数值仿真的方式验证其性能。为了产生随机实验数据, 参数 I 在 $[2,7]$ 随机产生, 参数 J 与参数 K 均在 $[10,15]$ 随机产生, 参数 T_L 设置为 50, 参数 L_k 在 $[10,50]$ 随机产生, 参数 λ_k 在 $[0,0.5]$ 随机产生, 参数 L_j 设置为 10, 参数 T_D 在 $[100,300]$ 随机产生。随机产生的实验场景中, 若针对服务链的端到端时延请求不存在可行的部署方案, 则该实验场景不纳入统计中。

3.2 结果分析

首先, 验证所搭建的原型系统面对安全事件时做出决策的时间。实验中预先在安全规则库内加入所要测试的安全事件规则, 再向系统中注入 5 种不同类型的危险流量, 结果如表 1 所示。可以看到, 系统发现安全事件并做出调整服务链决策的时间在 3 s 左右, 深入探索可以进一步发现实际上网络安全功能网元发现危险流量并告警的时间在毫秒级别, 系统所耗费的时间主要用于生成安全事件, 匹配安全规则库, 并做出调整服务链决策的过程。

表 1 发生安全事件后系统做出决策时间
Table 1 Time for the system to make decisions after security events

注入危险流量类型	系统决策时间/s
1	2.7
2	3.1
3	3.7
4	3.2
5	3.2

接着, 验证系统在做出决策后调整服务链部署的完成时间。实验发现该时间在 1 min~2 min。该时间跨度较大的原因为该时间与调整服务链过程中需要新增部署的 VNF 数量有关。若服务链调整部署过程中不需要新增部署 VNF, 则该调整过程能够在 3 s 内完成。若需要新增部署 VNF, 由于在 OpenStack 平台中新建虚拟机需要一定时间, 整体的调整时间变长。图 4 展示了新增部署 VNF 所需的时间与部署数量之间的关系, 可以看到当

新增部署 10 个以上 VNF 实例时, 所需的时间接近 1 min。从以上分析可以得出结论, 当需要系统快速做出服务链调整响应时, 可以提前新建 VNF 实例并保持运行, 但这种方式同时会造成资源开销增加。

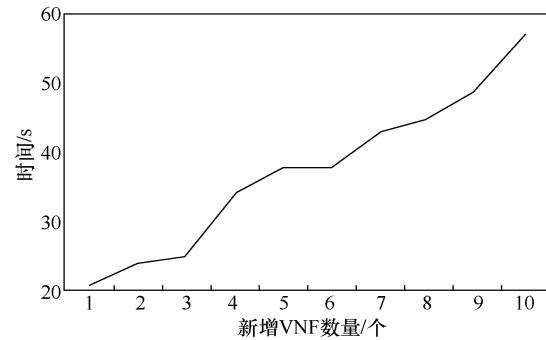


图 4 新增部署 VNF 所需的时间与部署数量之间的关系
Figure 4 The relationship between the time required for deploying VNF and the number of deployed VNF

最后, 验证本文所设计的服务链编排映射算法的性能。基于数值仿真中的参数设置, 本节对比了本文所设计的算法与一种随机部署算法的性能。随机部署算法随机选择服务链中网络功能的部署和映射方式, 并按照同样的方法推导计算满足服务链时延要求的 VNF 资源分配量。由图 5 所示的结果可知, 本文算法相比随机部署算法可节省 65% 的虚拟资源消耗, 这是因为本文算法优先选择 PNF 作为网络功能, 即使在选择 VNF 时, 也优先选择分配同样虚拟资源时能降低处理时延最多的 VNF。

4 结束语

本文设计了一种面向网络安全资源池的智能服务链系统。该系统构建了包含 PNF 网元与 VNF 网元的服务链, 并融入 SDN 技术实现系统的智能化管控, 能够基于对安全日志的检测结果调整服务链的部署形态, 提高网络安全系统的部署灵活度。同时, 本文设计了一种服务链的编排映射模型与算法, 应用于本文所设计的系统能够有效降低系统对虚拟资源的使用, 提高网络安全资源池内整体资源的使用效率。该系统有望运用于园区与数据中心网络出口处的网络安全区域^[21], 通过新增服务器运行 VNF, 以及新增 SDN 交换机连接 PNF 与服务器, 并应用该

系统实现对网络安全区域的改造, 简化该区域运维, 提高该区域的灵活度。

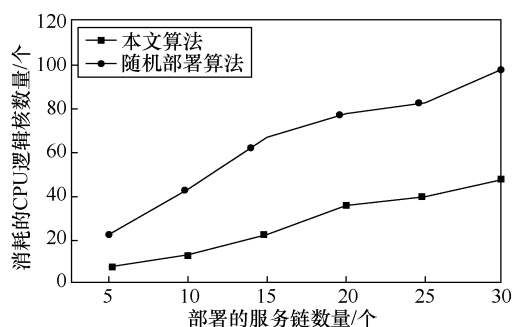
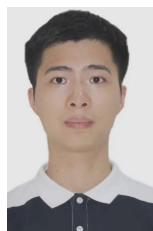


图5 各算法消耗虚拟资源量对比
Figure 5 Comparison of amount of virtual resources consumed by each algorithm

参考文献:

- [1] ZHANG X S, CHENG X Z, LI H B, et al. Security service chain based on sdn&nfv construction technology[C]//Signal and Information Processing, Networking and Computers. Lecture Notes in Electrical Engineering, vol 628. 2020.p.840-848.
- [2] ZHU S, ZHOU C, WANG C, Security service function chain based on software-defined security[J]. Journal of Physics: Conference Series, 2021. 2010(1): 12083.
- [3] KRISHNAN P, DUTTAGUPTA S, ACHUTHAN K. SDN/NFV security framework for fog to things computing infrastructure[J]. Software: Practice and Experience, 2020, 50(5): 757-800.
- [4] CHIOSI M, CLARKE D, WILLIS P, et al. Network functions virtualisation introductory white paper[R]. SDN and OpenFlow World Congress, 2012.
- [5] MCKEOWN N, ANDERSON T, BALAKRISHNAN H, et al. OpenFlow: Enabling innovation in campus networks[J]. ACM SIGCOMM Computer Communication Review, 2008, 38(2): 69-74.
- [6] LINA Z, DONGZHAO Z. A new network security architecture based on SDN/NFV technology[C]//2020 International Conference on Computer Engineering and Application (ICCEA). IEEE, 2020: 669-675.
- [7] SANTOS G L, BEZERRA D F, ROCHA E S, et al. Service function chain placement in distributed scenarios: a systematic review[J]. Journal of Network and Systems Management, 2022, 30(1): 1-39.
- [8] CHEN W, WANG Z, ZHANG H, et al. Cost-efficient dynamic service function chain embedding in edge clouds[C]//2021 17th International Conference on Network and Service Management (CNSM). IEEE, 2021: 310-318.
- [9] SHIN S, PORRAS P, YEGNESWARAN V, et al. FRESKO: modular composable security services for soft-ware-defined networks[C]//Proceedings of the 20th Annual Network and Distributed System Security Symposium. 2013.
- [10] LIU Y P, GUO Z G, SHOU G C, et al, To achieve a security service chain by integration of NFV and SDN[C]//2016 Sixth International Conference on Instrumentation & Measurement, Computer, Communication and Control (IMCCC). 2016: 974-977.
- [11] MARTINI B, PAGANELLI F, MOHAMMED A A, et al. SDN controller for context-aware data delivery in dynamic service chaining[C]//Proceedings 1st IEEE Conference on Network Softwarization, 2015: 1-5.
- [12] GIOTIS K, KRYFTIS Y, MAGLARIS V. Policy-based orchestration of NFV services in software-defined networks[C]//Proceedings of the 1st IEEE Conference on Network Softwarization. 2015. 1-5.
- [13] QAZI Z A, TU C C, CHIANG L, et al. SIMPLE-flying middlebox policy enforcement using SDN[C]//Proceedings of the ACM SIGCOMM 2013. 2013. 27-38.
- [14] IFFLANDER L, WALTER J, EISMANN S, et al. The "Vision of self-aware reordering of security network function Chains[C]// Companion of the 2018 ACM/SPEC International Conference on Performance Engineering. 2018.
- [15] 刘宇涛,陈海波. 虚拟化安全: 机遇, 挑战与未来[J]. 网络与信息安全学报, 2016, 2(10): 17-28.
LIU Y T, CHEN H B. Virtualization security: the good, the bad and the ugly[J]. Chinese Journal of Network and Information Security, 2016, 2(10): 17-28.
- [16] LI B, CHENG B, LIU X, et al. Joint resource optimization and delay-aware virtual network function migration in data center networks[J]. IEEE Transactions on Network and Service Management, 2021, 18(3): 2960-2974.
- [17] CERRATO I, ANNARUMMA M, RISSO F. Supporting fine-grained network functions through Intel DPDK[C]//2014 Third European Workshop on Software Defined Networks. 2014: 1-6.
- [18] MAHDAVIFAR S, GHORBANI A A. DeNNes: deep embedded neural network expert system for detecting cyber attacks[J]. Neural Computing and Applications, 2020, 32(18): 14753-14780.
- [19] LIU Y, LU Y, LI X, et al. On dynamic service function chain reconfiguration in IoT networks[J]. IEEE Internet of Things Journal, 2020, 7(11): 10969-10984.
- [20] 谢记超,伊鹏,张震,等. 基于异构备份与重映射的服务功能链部署方案[J]. 网络与信息安全学报, 2018, 4(6): 23-35.
XIE J C, YI P, ZHANG Z, et al. Service function chain deployment scheme based on heterogeneous backup and remapping[J]. Chinese Journal of Network and Information Security, 2018, 4(6): 23-35.
- [21] HUANG M, LUO W, WAN X. Research on Network Security of Campus Network[C]//Journal of Physics: Conference Series. IOP Publishing, 2019, 1187(4): 042113.

[作者简介]



王泽南 (1994-), 男, 浙江湖州人, 博士, 主要研究方向为网络功能虚拟化、网络智能。

李佳浩 (2001-), 男, 甘肃平凉人, 主要研究方向为软件定义网络。

檀朝红 (1985-), 男, 安徽安庆人, 主要研究方向为软件定义网络、云计算、网络功能虚拟化。

皮德常 (1971-), 男, 河南周口人, 南京航空航天大学教授、博士生导师, 主要研究方向为软件工程新技术、软件安全性测试方法。