基于智能服务链的数据中心安全架构重构的研究和实践

陈章迎，房一泉
（华东理工大学信息化办公室，上海 200237）

摘　要：随着园区数据中心安全设备日益增多（如网络防火墙、应用防火墙、数据库防火墙、入侵防御和检测系统等），如何在不影响设备功能和性能的前提下，更好地保护数据中心数据和资产的安全。基于此，以智能服务链为研究载体，通过部署安全资源池，重构数据中心安全架构，实施灵活流量编排，优化网络流量敏捷调度和智能控制，为网络安全设备智能化、个性化、差异化的部署提供实践支撑。

关键词：智能服务链；安全资源池；流量编排；智能控制
中图分类号：TP393
文献标志码：A
DOI：10.11959/j.issn.1000–436x.2024248

Research and practice on data center security architecture refactoring based on intelligent service chain

CHEN Zhangying, FANG Yiquan
Informazation of East China University of Science and Technology, Shanghai 200237, China

Abstract: With the increasing number of security devices in data centers, such as network firewalls, application firewalls, database firewalls, intrusion prevention and detection systems, it is worth researching and exploring how to better protect the security of data center data and assets without affecting device functionality and performance. Based on this, used intelligent service chain as the research carrier, by deploying secure resource pools, reconstructing data center security architecture, implementing flexible traffic orchestration, optimizing network traffic agile scheduling and intelligent control, practical support is provided for the intelligent, personalized, and differentiated deployment of network security devices.

Keywords: intelligent service chain, secure resource pooling, traffic orchestration, intelligent control

0　引言

智能服务链是以软件定义网络（SDN, software defined network）[1]和网络功能虚拟化（NFV, network function virtualization）[2]为技术基础，将传统网络安全设备由串接模式变更为并联模式，即实现物理旁挂、逻辑串接方式，构建安全设备资源池，实现流量调度和流量编排等智能化的服务链功能。重构边界网络为轻量化和扁平化的全新架构，提高边界网络的灵活性和可靠性，解决传统网络边界普遍存在的单点故障、性能瓶颈、灵活性差、运维复杂等问题，实现智能化、个性化、差异化的安全设备部署，整合资源并简化架构。

1　安全架构现状及分析

目前很多高校有多个校区，为确保异地数据访问的及时、可靠和稳定性，每个校区都会建设数据中心。为保证数据的安全，它们都会在各自数据中心出口串接诸如网络防火墙和应用防火墙等众多安全设备。伴随攻防等级的提升，相应的安全设备逐渐增多。图1为两校区数据中心网络架构拓扑，两校区在主干路由器和数据中心核心交换机之间串联网络防火墙和应用防火墙（WAF, web application fire-

收稿日期：2024–10–29

wall)，两校区之间以波分复用设备互联，实现数据传输。

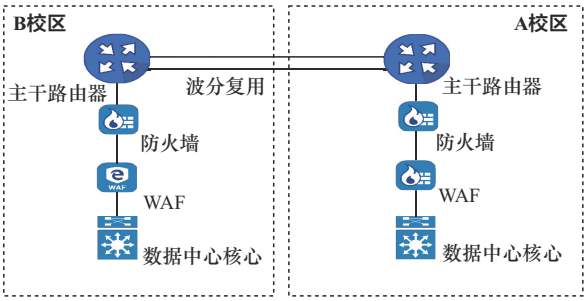


图1　两校区数据中心网络架构拓扑

从图1可知，随着校区数据中心的建设，每个中心机房需配备同比例的安全设备。同时，设备串联模式势必造成如下影响。1)安全架构与网络架构紧耦合。安全工具的部署与现网结构紧密关联，新业务上线、扩容或业务发生变更时，需手工修改转发路径下安全工具的策略，牵一发而动全身，无法满足业务快速迭代、变更的需求，无法为不同业务提供统一的差异化、个性化的安全策略。2)成本高，投入大。每个校区安全工具都是独立部署和单独采购，大多数情况下新购设备基于成本考虑无法统一型号，一定程度上又增加了管理、维护及备件成本。3)安全资源难以池化、扩展性差。安全资源串接部署模式，流量需经过各安全资源，不能基于具体业务需求提供差异化、个性化服务，部分业务流量因网络架构导致双重流量二次穿越相同资源。随着业务的增长安全资源往往成为性能瓶颈，一旦设备性能出现不足，就只能更换更高端的设备进行扩容。4）安全资源无法复用，利用率低。各校区数据中心安全设备采用主备或一主多备部署模式，无法实现流量的负载分担，且无法跨区域共享，设备利用率低下。

2　数据中心安全架构重构及分析

2.1　网络安全架构重构

为实现多校区数据中心安全设备安全架构和网络架构解耦，满足业务的快速迭代和变更需求，优化流量敏捷调度和智能化控制能力。同时，构建跨校区设备共享，提高资源利用率，合理控制投入成本，减轻和方便维护及管理。并且，将安全资源旁挂并实现逻辑串接形成资源池化，提供个性化、灵活及按需业务服务，分类实施安全策略。为此，本文引入基于SDN的智能服务链部署方式[3]，重构传统的3层安全架构模式，同类型安全设备构建相应的资源池[4]，旁挂在SDN交换机集群，SDN交换机集群由SDN控制器统一纳管[5]，实现控制管理和数据转发的分离，以软件方式实现网络流量编排的智能化和自动化，如图2所示。

由图2可知，某高校两校区安全架构经由智能服务链重新部署后，数据中心核心交换机和校区主干路由器通过SDN交换机集群互联，异地SDN集群经由波分复用设备互联以实现SDN控制器统一管理和集群化部署。由于网络出口链路及核心设备主要集中在A校区，为此，安全设备资源池相应集中规划并部署在A校区数据中心，并串接在SDN交换机集群内。通过整理并统一资源部署，实现同类设备的主备运行模式，构建网络防火墙资源池、

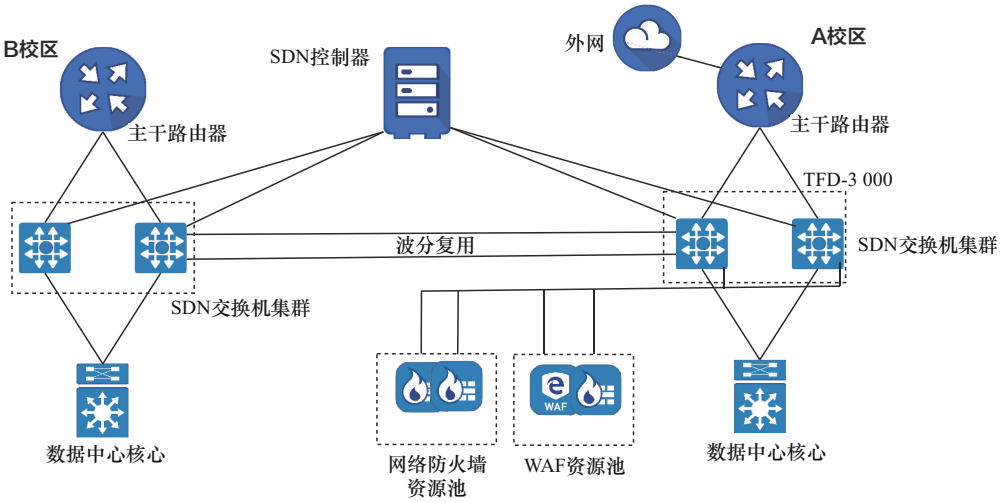


图2　安全架构重构拓扑

WAF 资源池 2 个安全资源池，后期可随业务的增加、扩容及更新等灵活扩容对应资源池，如安全套接层（SSL, security socket layer）资源池、入侵预防系统（IPS, intrusion prevention system）资源池、日志审计资源池等。B 校区流经数据中心的流量都会通过 SDN 交换机集群进入 A 校区安全资源池，然后再回流至 B 校区 SDN 交换机。通过这一设计，不仅简化了整个数据中心的安全架构，统一了流量管控，实现了智能化流量编排，也极大地降低了投入和维护成本，提升了安全资源利用率。同时，也实现了数据中心资源和数据的安全[6]。

2.2　智能服务链配置和实现

1) 管理地址及网关配置

配置智能服务链管理地址及网关

configure terminal

management ip address 172.20.6.198（设备管理 IP 地址配置）

management route add geteway 172.20.6.1（设备网络默认路由配置）

2) SDN 交换机添加至 SDN 控制器

将 SDN 交换机注册至智能服务链 SDN 控制器

#configure terminal

#openflow set controller mgmt tcp 172.20.5.218 6633（设置 SDN 控制器 IP 地址和端口号）

3) SDN 交换机集群高可靠性配置

配置聚合端口作为 SDN 交换机集群高可靠性（HA, high availability）互连接口，默认使用静态聚合配置。将指定接口添加至聚合接口

configure terminal

interface eth-0-X

no vlan-filter disable

no openflow enable

static-channel-group X

聚合接口下开启 openflow 转发配置

#interface aggX

#openflow enable

#vlan-filter disable

4) 智能服务链创建

创建高可靠性服务链，类型为 HA，数据封装模式 VLAN-PCP，选择指定接口作为内外网及 HA 接口。配置服务链黑白名单策略并创建服务链并开启，如图 3 所示。

按图 3 所示在 SDN 控制器平台内创建智能服务链，分别建立网络和应用防火墙 2 个安全资源池，具体拓扑如图 4 所示。其中 2 台 SDN 交换机通过端口捆绑（AGG1 和 AGG2）形成 HA 集群，实现主备灵活切换。网络防火墙（FW_01 和 FW_02）和应用防火墙（WAF_01 和 WAF_02）分别以主备模式串接在 SDN 交换机上，构成 2 个安全资源池，通过 Bypass 按钮可快速实现流量直通（跳过安全设备）及主备切换，以达到故障设备排查或设备更新。

2.3　业务流量验证

依据数据中心业务类型和整个安全防护策略规划，除 Web 服务器集群的流量（如图 5 黑色实线所示）需经 2 个安全资源池外，其他托管服务器集群、网络和管理服务器集群等（如图 5 黑色虚线所示）的流量通过网络防火墙资源池，以期实现个性化、差异化流量编排和调度。

为证实智能服务链的网络流量编排是否与规划和设计相符，本文在 SDN 控制器平台上对网络防火

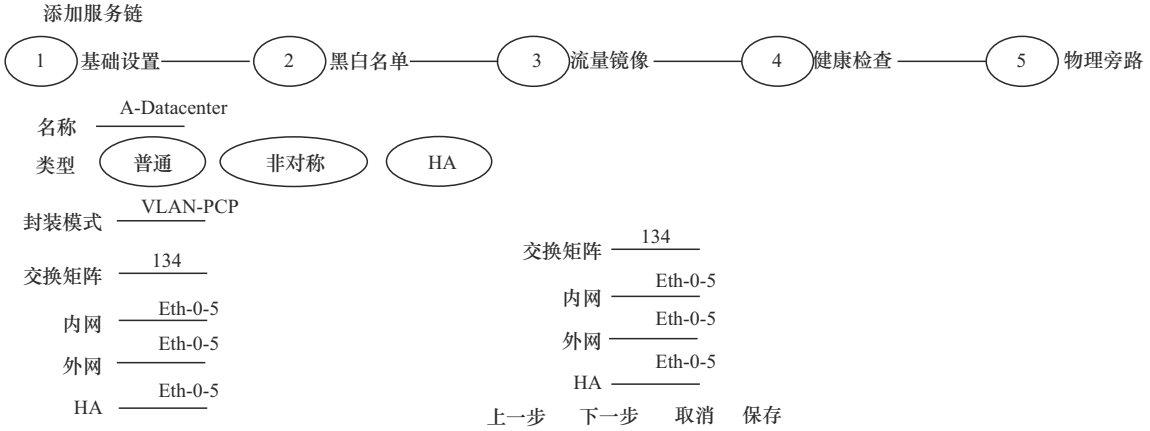


图3　智能服务链创建

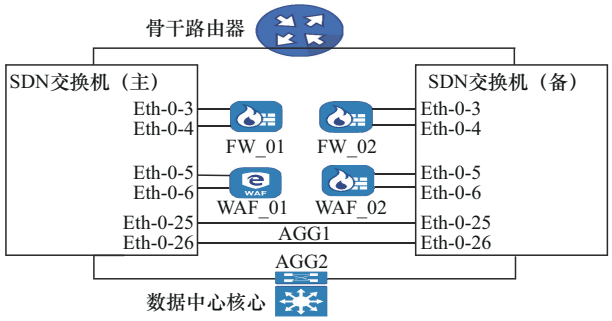


图4　智能服务链拓扑

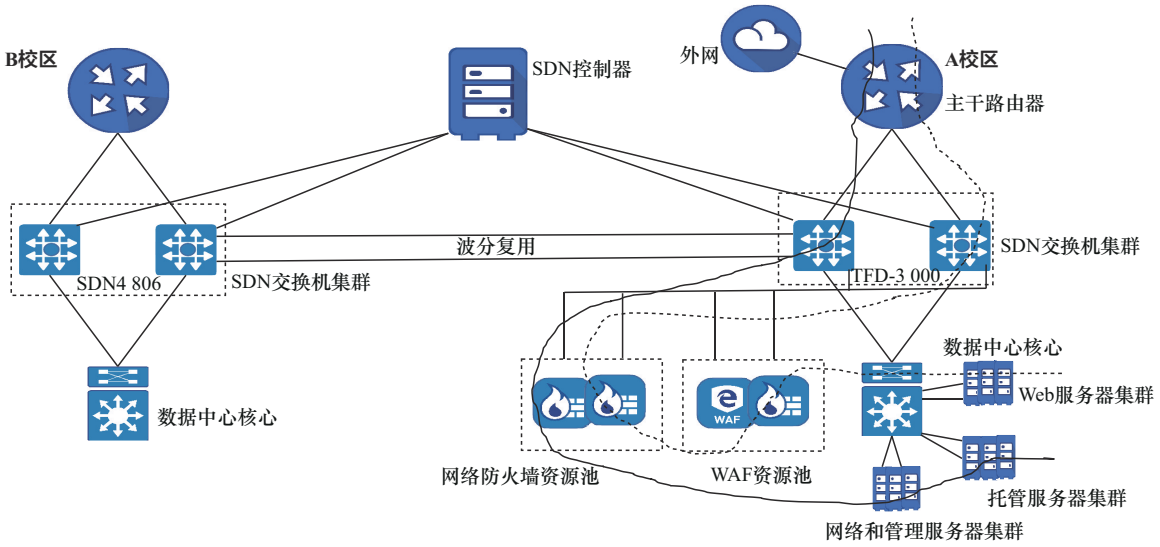


图5　服务器集群流量走向

墙和应用防火墙安全资源池实时流量监控（如图6所示）及业务测试和分析。结果表明，实际业务流量与设计相符，通过智能服务链可进行灵活流量编排和调度。同时，还可通过ByPass开关按钮灵活地放通或切换安全资源池内的主/备设备。

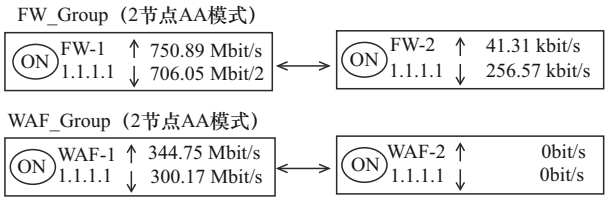


图6　智能服务链实时流量监控

SDN交换机集群的可靠性也是确保智能服务链流量调度的关键因素。为此，从主干路由器上对数据中心核心交换机的路径可达性进行探测，测试结果表明，在链路切换过程中，只丢失3个数据报文后，流量随即切换至备用SDN交换机，业务几乎不受任何影响。

```
lab@XH-Core-MX2008-B> ping 10.188.10.66
PING 10.188.10.66 (10.188.10.66): 56 data bytes
64 bytes from 10.188.10.66: icmp_seq=0 ttl=255 time=1.154 ms
64 bytes from 10.188.10.66: icmp_seq=1 ttl=255 time=1.003 ms
64 bytes from 10.188.10.66: icmp_seq=2 ttl=255 time=0.969 ms
64 bytes from 10.188.10.66
64 bytes from 10.188.10.66
64 bytes from 10.188.10.66
64 bytes from 10.188.10.66: icmp_seq=6 ttl=255 time=0.984 ms
64 bytes from 10.188.10.66: icmp_seq=7 ttl=255 time=1.010 ms
64 bytes from 10.188.10.66: icmp_seq=8 ttl=255 time=1.182 ms
64 bytes from 10.188.10.66: icmp_seq=9 ttl=255
```

time=0.903 ms

64 bytes from 10.188.10.66: icmp_seq=10 ttl=255 time=1.129 ms

64 bytes from 10.188.10.66: icmp_seq=11 ttl=255 time=1.030 ms

64 bytes from 10.188.10.66: icmp_seq=12 ttl=255 time=0.998 ms

64 bytes from 10.188.10.66: icmp_seq=13 ttl=255 time=0.982 ms

64 bytes from 10.188.10.66: icmp_seq=14 ttl=255 time=1.018 ms

64 bytes from 10.188.10.66: icmp_seq=15 ttl=255 time=1.916 ms

64 bytes from 10.188.10.66: icmp_seq=16 ttl=255 time=0.835 ms

64 bytes from 10.188.10.66: icmp_seq=17 ttl=255 time=0.796 ms

64 bytes from 10.188.10.66: icmp_seq=18 ttl=255 time=0.839 ms

64 bytes from 10.188.10.66: icmp_seq=19 ttl=255 time=0.871 ms

--- 10.188.10.66 ping statistics ---

20 packets transmitted, 17 packets received, 15% packet loss

round-trip min/avg/max/stddev = 0.796/1.060/1.916/0.259 ms

3　结束语

本文基于智能服务链将高校数据中心传统3层安全架构进行重构，构建以SDN控制器和SDN交换机集群为基础，形成安全资源池为框架的防御体系。在经过测试并实际部署于生产环境中，运行结果表明与规划设计基本一致。但在多校区跨区域流量调度及网络流量编排中也发现少许问题，比如SDN集群流量的采集、处理和分析等也存在亟须完善和优化。随着网络攻击事件的频次和严重性不断增加，引入人工智能技术[7-8]，通过大数据采集和分析，在威胁攻击前或攻击中提前识别后将其阻断，或者引流至蜜罐或者其他安全资源池用以进一步分析并加固安全设备。同时，随着IPv6规模化应用落地和终端普及，并将支持IP v6的安全设备作为智能化安全资源池一部分，智能化和自动化将IPv6威胁流量识别、分析和处理，这是后期值得研究和实践的一个方向。

参考文献：

[1] MCKEOWN N, ANDERSON T, BALAKRISHNAN H, et al. OpenFlow [J]. ACM SIGCOMM Computer Communication Review, 2008, 38(2): 69-74.

[2] CHIOSI M, CLARKE D, WILLIS P, et al. Network functions virtualisation introductory white paper[R]. 2012.

[3] 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.
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.

[4] 孙磊, 孙淑昕, 王博文, 等. 煤矿企业数据中心网络安全服务链技术研究[J]. 工矿自动化, 2022, 48(7): 149-154.
SUN L, SUN S X, WANG B W, et al. Research on network security service chain technology of data center in coal mine enterprise[J]. Journal of Mine Automation, 2022, 48(7): 149-154.

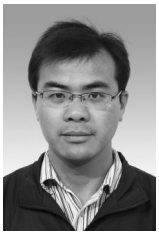
[5] 中通服咨询设计研究院有限公司. 一种基于SDN技术的网络流量编排系统和方法: CN201710639898.0[P]. 2019.
Zhongtongfu Consulting Design and Research Institute Co., Ltd. A network traffic orchestration system and method based on SDN technology CN201710639898.0[P]. 2019.

[6] HUANG M, LUO W B, WAN X. Research on network security of campus network[J]. Journal of Physics: Conference Series, 2019, 1187(4): 042113.

[7] 陈天骄, 刘江, 黄韬. 人工智能在网络编排系统中的应用[J]. 电信科学, 2019, 35(5): 9-16.
CHEN T J, LIU J, HUANG T. Application of artificial intelligence in network orchestration system[J]. Telecommunications Science, 2019, 35(5): 9-16.

[8] YUSOF M A M, ALI F H M, DARUS M Y. Detection and defense algorithms of different types of DDoS attacks using machine learning[C]//International Conference on Computational Science and Technology. Berlin: Springer, 2018: 370-379.

[作者简介]



陈章迎（1980– ），男，江西泰和人，华东理工大学工程师，主要研究方向为计算机网络、计算机应用、信息安全和智能交通系统。

房一泉（1975– ），女，江苏扬州人，华东理工大学高级实验师，主要研究方向为大数据分析与机器学习等。