



研究与开发

面向服务的数据中心安全框架

胡腾¹, 李观文², 周华春²

(1. 中国工程物理研究院计算机应用研究所, 四川 绵阳 621900;

2. 北京交通大学电子信息工程学院, 北京 100044)

摘要: 随着数据中心网络在云计算领域的大规模商用, 数据网络的安全问题愈发受到重视。然而, 由于传统数据中心安全设备部署方式静态僵化, 难以满足动态多变的网络安全态势, 无法应对新的安全威胁。因此, 提出一种面向服务的数据中心安全框架。基于虚拟化技术和软件定义网络, 将虚拟化的安全功能灵活组合, 并实现安全策略动态更新的过程。通过原型系统测试验证了所提安全框架的可行性和有效性, 为数据中心网络的灵活性和安全性提升提供了一种解决方案。

关键词: 数据中心网络; 安全功能链; 安全策略部署

中图分类号: TP393

文献标识码: A

doi: 10.11959/j.issn.1000-0801.2018031

Service-oriented security framework for datacenter networks

HU Teng¹, LI Guanwen², ZHOU Huachun²

1. Institute of Computer Application, China Academy of Engineering Physics, Mianyang 621900, China

2. School of Electronic and Information Engineering, Beijing Jiaotong University, Beijing 100044, China

Abstract: With the large-scale deployment of datacenters in cloud computing, there is an increasing attention to their security issues. However, with the ossify deployment of traditional security devices, it is hard to meet the requirements of dynamical network security situation and copy with new kinds of security threats. Therefore, a service-oriented security framework for datacenter networks was proposed, which was able to compose the virtualized security functions flexibly and update the security policies dynamically based on virtualization technology and software-defined networking. With the implementation of prototype, the feasibility and availability of the proposed security framework was proved, and a solution to promote the flexibility and security of datacenter networks was provided.

Key words: datacenter network, security function chaining, security policy deployment

收稿日期: 2017-11-14; 修回日期: 2017-12-13

基金项目: NSAF 联合基金资助项目 (No. U1530118); 国家自然科学基金资助项目 (No. 61271202); 国防基础科研基金资助项目 (No. JCKY2016212C005)

Foundation Items: NSAF (No. U1530118), The National Natural Science Foundation of China(No. 61271202), National Defense Basic Scientific Research Program of China(No. JCKY2016212C005)

1 引言

随着云计算的发展与普及,数据中心规模化增长的需求与日俱增。但是,当前网络安全态势十分严峻,数据中心网络面临的安全威胁更是不容忽视。Cisco 2017 数据中心安全研究报告^[1]指出,88% 的数据中心管理者称 2016 年收到的安全攻击有所增多,而只有 38% 的管理者认为数据中心应对安全威胁的能力较好。面对不断增多的安全威胁,数据中心网络需要更加灵活和动态的安全保障方案。

然而,面对复杂的网络安全局势,一方面,传统数据中心安全设备集成度高、安装部署复杂、更新成本大等局限,导致其难以有效应对新的安全威胁和更多样化的安全需求^[2];另一方面,云计算的应用带来更加个性化的用户服务,也对数据中心安全提出更高的要求,过去静态僵化的安全服务将无法未来满足未来数据中心网络动态灵活的安全需求^[3,4]。因此,需要建立面向服务的数据中心按需安全框架。

逐渐成熟的 NFV(network function virtualization, 网络功能虚拟化)技术^[5]结合 SDN (software-defined networking, 软件定义网络)^[6],可以实现对网络流量的灵活调度与网络资源的动态组合。参考文献[7]由此提出了一种移动目标防御框架,实现灵活的数据中心安全防护,可以有效缓解多种安全攻击。参考文献[8]则基于 SDN 架构提出一种分析网络流量安全需求并部署相应安全功能的框架。直到 SFC (service function chaining, 服务功能链)工作组^[9]提出一种基于 SDN/NFV 的服务功能链架构,将现有的基础网络功能进行有序组合,首先提出在数据中心部署安全功能链^[10],以满足未来数据中心网络更加灵活、多样化的安全需求。参考文献[11]综合考虑了当前网络面临的主要安全威胁,总结了 12 种基本的网络安全防御模式,提出针对不同类型安全威胁的安全功能链构

建方式,现已经基本实现常见安全场景的覆盖。参考文献[12]进一步将 SFC 的设计思想融入数据中心安全防护,通过动态调整流量的安全检测路径,适应用户动态的安全需求。然而,为应对新的安全威胁,除了安全功能的动态组合,还需要安全策略的快速部署与及时更新。I2NSF (interface to network security function, 网络安全功能接口)工作组^[13]提出一种安全策略部署框架,期望实现安全策略动态按需的管理,可以为数据中心网络的安全管理员提供更加便捷、灵活的安全策略管理模式,有效降低安全策略,更新成本。然而,目前尚缺乏一种统一的数据中心安全框架,可以同时实现安全功能的灵活组合与安全策略的动态更新。

因此,本文结合 I2NSF 与 SFC 的设计思想,提出一种面向服务的数据中心安全框架。该架构将传统的基础安全功能进行虚拟化与资源池化,同时解耦控制层面与数据转发层面,可以针对不同安全威胁灵活组合所需的安全功能,有效降低安全功能重新部署的成本,并支持数据中心网络动态可变的安全需求。同时,采用面向服务的策略管理方法,降低数据中心网络安全维护成本和网络管理员的操作复杂度,从而提高策略配置的效率 and 正确性。

2 面向服务的安全框架

本框架采用虚拟化技术,将传统网络安全功能资源池化,实现对网络中安全服务资源的统一管理和灵活调度。该框架基于安全功能链思想,根据用户业务的特定需求,将多种安全功能进行链式组合,并根据需要在各安全功能上部署相应的安全策略,动态构建所需的安全功能链。此外,考虑到用户业务可能经过分布式的多数据中心结构,该框架可实现跨域的安全互联,同时保障用户侧和数据侧的安全。提出的面向服务的安全框架设计如图 1 所示。

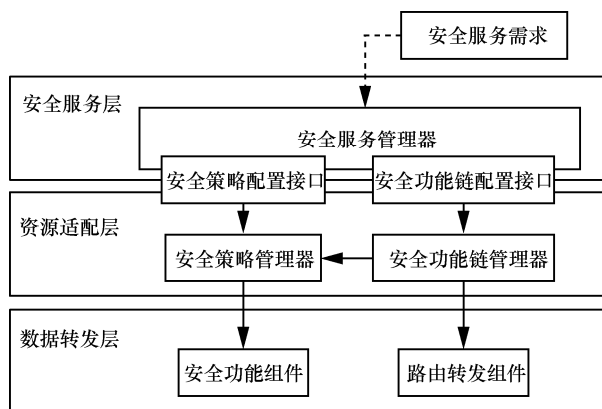


图1 面向服务的安全框架设计

2.1 安全服务层

安全服务层致力于满足网络安全管理员的安全服务需求,并针对这些安全服务需求进行安全服务的分类与安全策略的分配,确定网络安全管理员所需的逻辑安全功能链。安全服务管理器实现从安全服务需求到逻辑安全功能链及相应安全策略的匹配过程。

安全服务需求可以由网络安全管理员手动配置,即先通过安全功能配置界面设定所需的安全功能,然后,跳转到安全策略配置界面,根据安全功能的类型制定相应的安全策略。安全服务管理器根据网络安全管理员的配置生成逻辑的安全功能链,通过安全功能链配置接口交付给资源适配层的安全功能链管理器,安全策略则通过安全策略配置接口交付给安全策略管理器做进一步处理。

2.2 资源适配层

资源适配层从安全服务层获得网络安全管理员所需的逻辑上的安全功能链与安全策略,然后,分别交付给安全功能链管理器与安全策略管理器。其中,安全功能链管理器由安全适配模块、容器管理模块及流表管理模块组成。

安全适配模块首先解析安全服务层的逻辑安全功能链,匹配系统可提供安全功能实例资源,获知所需安全功能的类型与具体数量,然后,向容器管理模块发起资源请求。容器管理模块可以

基于当前网络系统的运行状态(如计算节点的CPU利用率和链路拥塞情况)和已开启的安全功能实例资源的负载状态信息,选择创建新的安全功能实例或重用已有安全功能实例。之后,容器管理模块会返回所请求的安全功能实例的相关信息(如网络位置信息)给安全适配模块。安全适配模块由此构建完整的网络拓扑信息,并通告流表管理模块。流表管理模块据此建立该安全功能链对应的完整的安全功能路径配置信息。此外,容器管理模块还可以动态调整安全功能实例资源,及时释放空闲的网络系统资源,提供系统资源的利用率。

安全策略管理器包括安全控制器和规则分发器,实现从面向用户的安全策略向面向功能的安全规则转换的翻译过程与规则下发过程。面向用户的安全策略由网络安全管理员进行配置,采用人类可读的语言描述,却无法直接由安全功能实例执行,因此,需要安全控制器对其进行一次策略翻译,实现从面向用户的安全策略到面向功能的安全规则的转换过程。与此同时,安全策略管理器也会收到来自安全功能链管理器分配的安全功能实例的相关信息,以生成实际可部署的安全规则,并调用规则分发器下发这些安全规则到对应的安全功能实例。

此外,资源适配层需要维护两个数据库,即安全功能信息库(security function information base, SFIB)和安全策略信息库(security policy information base, SPIB)。安全功能信息库存储网络中所有的安全功能实例资源的相关信息,用于容器管理模块动态查询与更新。安全策略信息库存储所有的安全策略信息,并维护面向用户的安全策略与面向功能的安全规则之间的映射关系。

2.3 数据转发层

数据转发层由两类实体组成,分别是安全功能组件和路由转发组件。

安全功能组件由容器管理模块动态维护,负

责提供安全功能实例资源。安全功能实例基于资源适配层的安全策略管理器下发的安全规则，对数据流执行实际的安全处理。

路由转发组件是数据流的基础转发设备，根据资源适配层的流表管理模块下发的流表信息，对数据流执行路由转发操作。路由转发组件包括分类器与转发器。其中，分类器负责对不同数据流标记相应的 SPI（service path ID，服务路径标识）并分配初始的 SI（service index，服务索引值），而转发器负责将数据流导入相应的安全功能实例，并对经过安全处理的数据流的 SI 执行减一操作。

3 关键技术

该框架涉及的关键技术包括安全功能的灵活组合与安全策略的动态部署两部分，分别介绍实现对应功能的安全功能链管理系统与安全策略管理系统。

3.1 安全功能链管理系统

安全功能链管理系统涉及安全服务层的安全需求配置界面、资源适配层的安全功能链管理系统与数据转发层的安全功能组件与路由转发组件。安全需求配置界面基于 OpenDaylight SFC 项目^[14]实现。

安全功能链管理器是面向服务的数据中心安全框架中控制平面的重要组成部分，实现虚拟网络资源的动态管理与适配、安全功能实例的按需选择或实例化、安全功能路径的动态创建与管理。安全功能链管理器的模块组成如图 2 所示。

安全功能链管理系统由安全适配模块、容器管理模块及流表管理模块组成。由于虚拟化的安全功能采用容器技术实现，对应的容器管理模块采用 Docker Swarm 技术^[15]管理网络中可用的安全功能资源。Docker Swarm 采用 TCP 与基础设施网络中的安全功能组件（计算节点）组成集群，同时为安全适配模块提供了系统调用的接口。流表管理模块基于 OpenDaylight SFC 项目开发，它

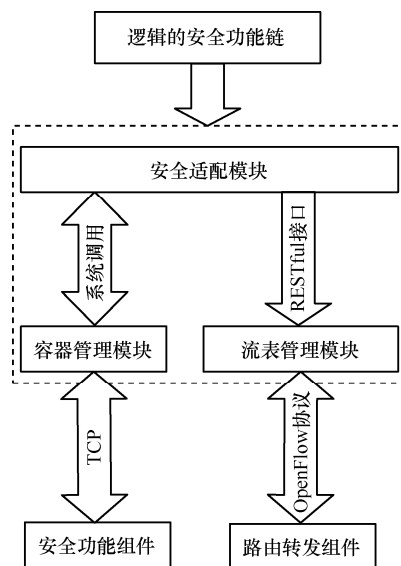


图 2 安全功能链管理系统设计

采用 OpenFlow 协议管理数据转发层中的路由转发组件，支持网络安全管理员通过 Web 界面配置逻辑安全功能链，同时也为安全适配模块提供了 RESTful 接口调用。考虑实际的安全功能链可能跨越多个数据中心域，扩展了 OpenDaylight SFC 的跨域互联功能，可生成跨域的转发流表。基于 Python 开发了安全适配模块，它一方面负责从安全服务层获得用户或网络安全管理员所需的逻辑上的安全功能链；另一方面，支持 Docker Swarm 与 OpenDaylight SFC 之间的通信与信息交互。

安全功能链管理系统的工作流程如下。

(1) 网络管理员通过安全需求配置界面定制所需的安全服务，生成逻辑的安全功能链。

(2) 安全适配模块采用系统调用的方式向容器管理器请求提供相应的安全功能实例，后者基于当前的资源信息，选择已有的安全功能实例或创建新的安全功能实例，并返回所选实例的网络信息。

(3) 安全适配模块调用 RESTful 接口向流表管理模块通告该安全功能链的转发配置。

(4) 流表管理模块利用 OpenFlow 协议向数据转发层中的安全感知组件和路由转发组件下发流表配置。



安全功能链管理系统的主要优势如下。

(1) 支持安全功能的虚拟化及对应实例的管理选择

数据转发层采用容器技术实现安全功能的轻量虚拟化, 安全功能链管理器中容器管理模块负责对这些虚拟化的安全功能实例进行统一管理。容器管理模块可以远程管理和控制每个计算节点的虚拟资源, 根据系统运行状态和负载状态动态创建、删除安全功能实例。安全适配器可以调用容器管理模块选择所需的安全功能实例。

(2) 支持数据中心域内的安全功能链自动化部署

安全功能链管理器的安全适配模块可以获得网络拓扑信息并告知流表管理模块, 由流表管理模块根据安全功能链的路径生成对应的转发流表, 下发到数据转发层。数据转发层的路由转发组件采用 Open vSwitch 软件交换机^[16]实现, 可以实现安全功能链中的分类器与转发器。通过安全功能链管理器下发流表到 Open vSwitch, 可以实现数据中心域内安全功能链的自动化部署。

(3) 支持跨数据中心域的安全功能链部署

扩展数据携带的头部信息, 可存储数据流跨数据中心域转发时所需的 SPI/SI 信息, 并扩展 OpenDaylight SFC, 实现控制层面对跨域转发逻辑的支持。通过预定义跨域所需的 SPI/SI 信息, 可以支持在多数据中心域中自动化部署安全功能链。

3.2 安全策略管理系统

安全策略管理系统涉及安全服务层的安全策略配置界面、资源适配层的安全策略管理器和数据转发层的安全功能组件。

安全策略管理器基于 I2NSF 控制平面设计, 可以实现网络安全管理员通过 Web 界面手动配置具体的安全策略, 并通过安全控制器下发到格式化的策略到制定的安全功能组件。安全策略管理器的基本工作流程如图 3 所示。

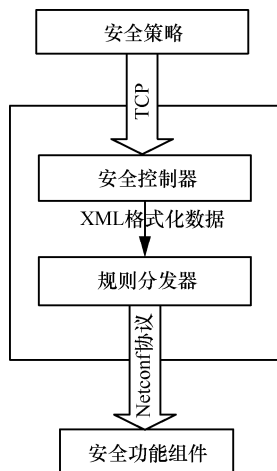


图3 安全策略管理系统设计

安全策略管理系统由用户界面和安全控制器组成。用户界面为网络安全管理员提供可视化的安全策略配置界面, 可指定所需安全服务类型与策略。安全控制器实现面向用户的安全策略到面向功能的安全规则的翻译过程, 并实现安全规则的自动化下发过程。

安全策略管理系统的工作流程如下。

(1) 网络安全管理员通过 Web 界面制定特定安全功能的安全策略, 将策略存入安全策略信息库, 同时发送给安全控制器。

(2) 安全控制器根据安全功能链管理器提供的安全功能实例信息, 将收到的面向服务的安全策略翻译为面向功能的安全规则, 并对其进行 XML 格式化。

(3) 安全控制器调用规则分发器将格式化的策略配置通过 Netconf 协议发送到安全功能实例上。

安全策略管理系统的主要优势如下。

(1) 支持动态策略更新

因为静态设置的数据编号, 过去同一安全对象的安全策略无法进行更新, 而这将不利于本地的策略维护与多域策略协同处理。因此, 应采用时间相关函数为安全策略分配动态编号, 初步实现本地策略更新功能。

(2) 支持多数据库同步

考虑多域安全策略共享与查询问题, 控制平

面采用可集群部署的数据库存储域内的安全策略。由于 Redis 数据库^[17]可以快速实现集群的部署且拥有较好的数据同步功能,因此,应选用 Redis 数据库作为安全策略数据库。

4 系统验证

为验证提出的面向服务的数据中心安全框架,本文基于 OpenStack^[18]建立虚拟化的测试床,参考 SFC 工作组草案^[10]给出的多数据中心环境下的多 SFC 域互联场景,建立如图 4 所示的系统验证场景。

该场景中,数据中心 1 构成一个云办公平台,可以为不同用户提供定制化和安全的云办公环境。而数据中心 2 通过虚拟化技术整合底层设施资源,可以为多个用户同时提供应用层服务。每个数据中心域内采用 SDN/NFV 技术搭建传统数据中心网络的 fat-tree 拓扑。由于两数据中心地理位置相距较远,数据中心 1 的用户可通过互联网

远程访问数据中心 2 中的服务资源。假定某一云办公平台用户希望访问位于数据中心 2 中的某种特定服务资源,则该用户的数据请求与传输需要跨域两个不同的数据中心。为保障整个通信过程的安全,需要为该用户的服务流建立一条跨域的安全功能链。其中,每个数据中心的接入层和汇聚层的虚拟交换机与核心层交换机均可视为转发器,入口/出口网关作为分类器,而安全功能实例则通过容器方式在虚拟交换机上按需开启。该场景中的安全功能链需要跨两个数据中心域,同时,保护用户侧和数据侧安全。其中,用户侧包括用于流量监控的入侵检测系统和进行内部防护的防火墙,数据侧则包含阻止外部入侵的防火墙与用于 DDoS 攻击缓解的入侵检测服务。两侧安全功能实例分别部署在靠近用户侧和数据侧的虚拟交换机上。

为验证提出的面向服务的数据中心安全框架,首先,通过安全服务管理器的配置界面部署

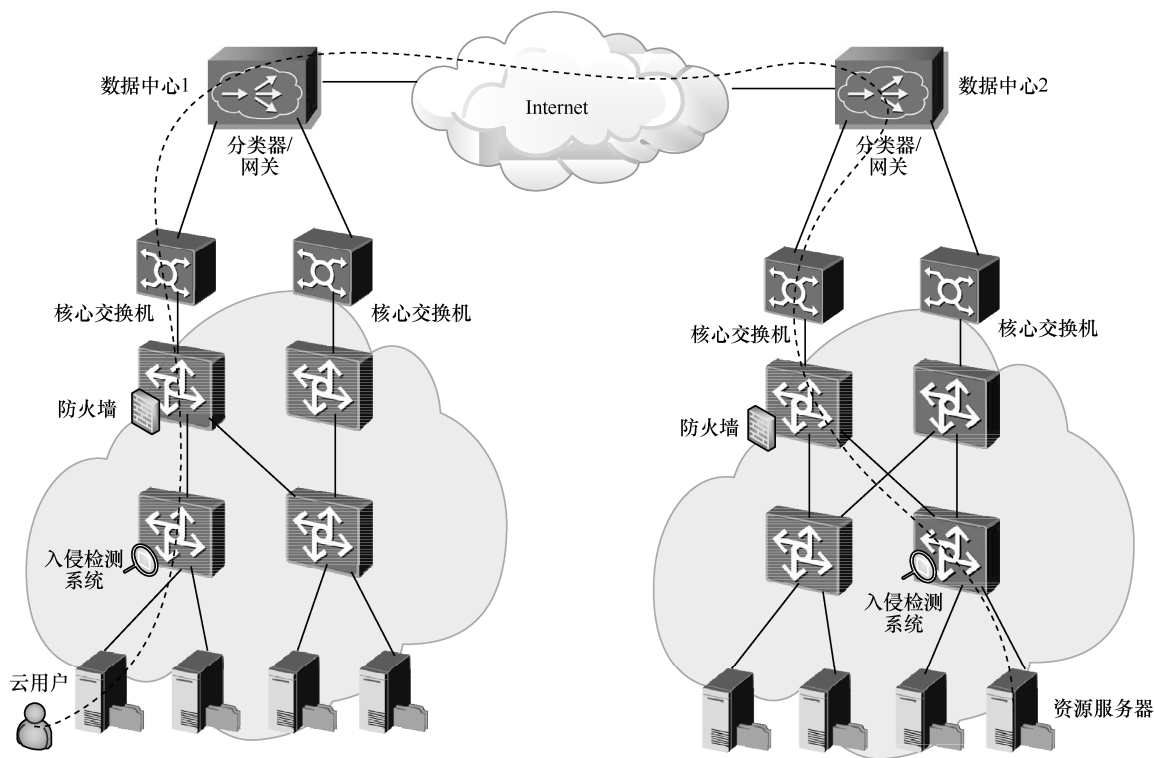


图 4 系统验证场景



该安全功能链，包括两个防火墙（FW）功能与两个入侵检测（IDS）功能。其中，左侧的防火墙与入侵检测系统位于数据中心 1，右侧的防火墙与入侵检测系统位于数据中心 2。安全功能链管理器根据安全需求分配安全功能链，并自动生成相应的 SPI 为 165，如图 5 所示。其中，防火墙功能由 iptables 软件^[19]实现，入侵检测功能由 Snort 软件^[20]实现。

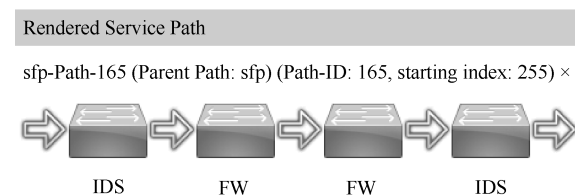


图 5 安全功能链配置界面

通过安全功能链管理系统对该安全功能链进行解析，并下发相应流表到对应的虚拟交换机上，以深度分组检测为例，其流表配置如图 6 所示。

```
cookie=0x14,duration=5238.972s,table=0,n_packets=10310,n_bytes=1402160,idle_age=0,priority=5
actions=resubmit(1)
cookie=0x14,duration=5238.972s,table=1,n_packets=8740,
n_bytes=1188640,idle_age=0,priority=250,ns=165,actions=resubmit(4)
cookie=0x14,duration=5238.943s,table=4,n_packets=4350,n_bytes=597040,idle_age=0,priority=550,nsi=255,
nsp=165,actions=load:0xac110002->NXM_NX_TUN_IPV4_DST[],resubmit(10)
cookie=0xba5eba1100000101,duration=5238.959s,table=10,n_packets=4390,n_bytes=597040,idle_age=0,pri
ority=655,nsi=255,ns=165,in_port=1,actions=move:NXM_NX_NSH_MDTYPE[]->NXM_NX_MDTYPE[],move:NX
M_NX_NSH_NPI[],move:NXM_NX_NSH_C1[]->NXM_NX_NSH_C1[],move:NXM_NX_NSH_C2[]->NXM_NX_NSH_C2[],
move:NXM_NX_NSH_C3[]->NXM_NX_NSH_C3[],move:NXM_NX_NSH_C4[]->NXM_NX_NSH_C4[],move:NX
H_NX_TUN_ID[0..31]->NSH_NX_TUN_ID[0..31],load:0x4->NXM_NX_TUN_GPE_NPI[],IN_PORT
```

图 6 将数据流导入入侵检测功能的流表项

从图 6 中可以看到，交换机接收到数据流后，通过流表逐条匹配 SPI 为 165（流表项中表示为 nsp）且 SI 为 255（流表项中表示为 nsi）的数据流。由于 255 为 SI 初始值，可以获知需要该数据流需要经过第一个安全功能，即入侵检测功能。然后匹配最终的流表条目，通过基于 NSH（network service header，网络服务报头）的 SFC 流转发方式^[21]，将数据流转发到入侵检测功能实例中。类似地，由于经过入侵检测功能处理后的数据流的 SI 值会减一（即 SPI 仍为 165，SI 为 254），通过匹配如图 7 所示流表，以类似方式转发数据

流至下一跳交换机。

```
cookie=0x14,duration=5238.972s,table=0,n_packets=10310,n_bytes=1402160,idle_age=0,priority=5
actions=resubmit(1)
cookie=0x14,duration=5238.972s,table=1,n_packets=8740,
n_bytes=1188640,idle_age=0,priority=250,ns=165,actions=resubmit(4)
cookie=0x14,duration=5238.943s,table=4,n_packets=4350,n_bytes=591600,idle_age=0,priority=550,nsi=254,n
sp=165,actions=load:0xac110002->NXM_NX_TUN_IPV4_DST[],resubmit(10)
cookie=0xba5eba1100000101,duration=5238.959s,table=10,n_packets=4350,n_bytes=591600,idle_age=0,pri
ority=655,nsi=254,ns=165,in_port=1,actions=move:NXM_NX_NSH_MDTYPE[]->NXM_NX_MDTYPE[],move:NXM
_NX_NSH_NPI[],move:NXM_NX_NSH_C1[]->NXM_NX_NSH_C1[],move:NXM_NX_NSH_C2[]->NXM_NX_NSH_C2[],
move:NXM_NX_NSH_C3[]->NXM_NX_NSH_C3[],move:NXM_NX_NSH_C4[]->NXM_NX_NSH_C4[],move:NX
H_NX_TUN_ID[0..31]->NSH_NX_TUN_ID[0..31],load:0x4->NXM_NX_TUN_GPE_NPI[],IN_PORT
```

图 7 处理从入侵检测功能流出数据的流表项

安全功能链系统通过解析网络安全管理员配置的安全需求，自动向每个转发器下发类似的流表，从而实现数据流在整个安全功能路径内的转发操作，确保数据流可以依次经过每个所需的安全功能实例。

安全功能链确定后，还要根据安全需求设定相应的安全策略。以该安全功能链中的入侵检测功能为例，首先，通过安全策略配置界面中的安全功能选择页面，选择需要配置策略的安全功能的类型，如图 8 所示。

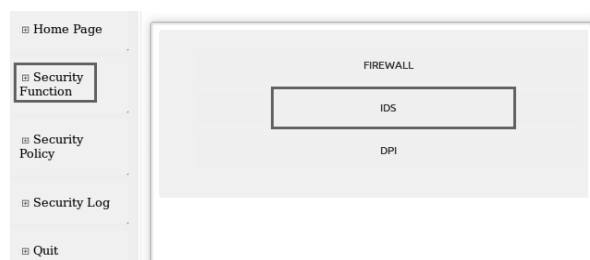


图 8 安全功能选择界面

然后，可以看到如图 9 所示安全策略详细配置界面。在这里，网络安全管理员可以定义该策略的名称、策略的匹配项目和所需要执行的安全行为。对于入侵检测功能，这里定义检测到源 IP 地址为 10.0.0.24 的数据流后进行告警操作。

配置好后选择提交，即可完成该功能的策略配置过程，后续的策略翻译与下发均由安全策略管理系统自动完成。其中，安全策略管理系统基于 Cisco 的 ConfD 引擎^[22]实现 Netconf 协议传输配置好的策略，在安全功能实例上可以实时看到

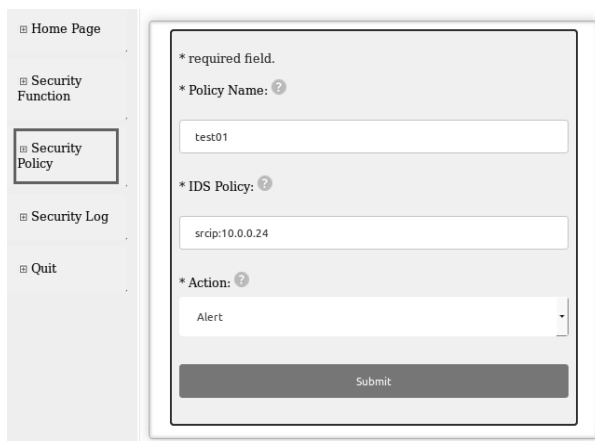


图 9 入侵检测配置界面

策略接收过程,如图 10 所示。此外,其他安全功能的策略配置过程也是类似的,此处不再赘述。

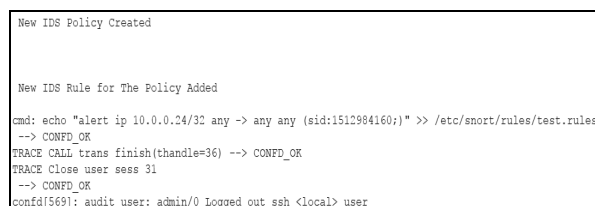


图 10 入侵检测功能实例的策略接收过程

此外,还可以通过如图 11 所示的安全功能日志选项,查看已配置好的安全策略,为网络安全管理员后续添加或修改安全策略做参考,避免错误配置或重复配置。



图 11 安全策略配置日志

最后,配置好的入侵检测系统策略被部署到入侵检测功能实例上。由于本文采用的入侵检测功能实例由 Snort 实现,可以看到如图 12 所示的 Snort 规则文件中存在新配置的条目,证明该安全策略已成功配置。

```
#-----
# TEST RULES
#-----
#
alert udp 10.0.0.28/32 any -> 10.0.0.27/32 any (msg:"Outer IP!";sid:10000001;)
alert ip 10.0.0.10/32 any -> 10.0.0.23/32 any (msg:"Inner IP!";sid:10000002;)
alert ip 10.0.0.24/32 any -> any any (sid:1459732485;)
```

图 12 入侵检测功能的规则文件

5 结束语

本文考虑到现有数据中心网络静态僵化的安全部署方案难以有效地应对日趋多样化的安全威胁,提出一种面向服务的数据中心网络安全框架,将网络安全功能进行虚拟化后统一管理;设计相应的安全功能管理与安全策略下发系统,以实现安全功能的灵活组合与安全策略的动态更新。通过原型系统测试,验证提出的安全框架可以满足未来数据中心网络更加灵活、个性的安全需求。

参考文献:

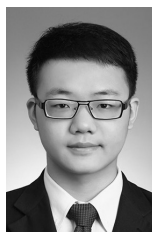
- [1] Cisco. Cisco Data Center Security Study[R]. 2017.
- [2] 韦乐平. SDN 的战略性思考[J]. 电信科学, 2015, 31(1): 7-12.
WEI L P. Strategic thinking on SDN [J]. Telecommunications Science, 2015, 31(1): 7-12.
- [3] 王歆平, 王茜, 刘恩慧, 等. 基于 SDN 的按需智能路由系统研究与验证[J]. 电信科学, 2014, 30(4): 8-14.
WANG X P, WANG Q, LIU E H, et al. Research and verification on SDN-based on-demand smart routing system [J]. Telecommunications Science, 2014, 30(4): 8-14.
- [4] 李丹, 刘方明, 郭得科, 等. 软件定义的云数据中心网络基础理论与关键技术[J]. 电信科学, 2014, 30(6): 48-59.
LI D, LIU F M, GUO D K, et al. Fundamental theory and key technology of software defined cloud data center network [J]. Telecommunications Science, 2014, 30(6): 48-59.
- [5] HAN B, GOPALAKRISHNAN V, JI L, et al. Network function virtualization: challenges and opportunities for innovations[J]. IEEE Communications Magazine, 2015, 53(2): 90-97.
- [6] NICK M, TOM A, HARI B, et al. OpenFlow: enabling innovation in campus networks[J]. ACM SIGCOMM Computer Communication Review, 2008, 38(2): 69-74.
- [7] CHUNG C J, XING T, HUANG D, et al. SeReNe: on establishing secure and resilient networking services for an SDN-based multi-tenant datacenter environment[C]// IEEE International Conference on Dependable Systems and Networks Workshops, June 22-25, 2015, Rio de Janeiro, Brazil. Piscataway: IEEE Press, 2015.
- [8] AMMAR M, RIZK M, ABDEL-HAMID A, et al. A framework for security enhancement in SDN-based datacenters[C]//2016



- 8th IFIP International Conference on New Technologies, Mobility and Security, November 21-23, 2016, Larnaca, Cyprus. Piscataway: IEEE Press, 2016.
- [9] JOEL H, CARLOS P. Service function chaining, RFC Editor, October 2015[R/OL]. (2015-10-01)[2017-11-14]. <https://www.rfc-editor.org/rfc/rfc7665.txt>.
- [10] KUMAR S, TUFAIL M, MAJEE S, et al. Service function chaining use cases in data centers. Internet-Draft draft-ietf-sfc-dc-use-cases-06[RB/OL]. (2017-01-01)[2017-11-14]. <http://www.ietf.org/internet-drafts/draft-ietf-sfc-dc-use-cases-06.txt>.
- [11] LEIVADEAS A, FALKNER M, LAMBADARIS I, et al. Resource management and orchestration for a dynamic service chain steering model[C]//IEEE Global Communications Conference, December 4-8, 2016, Washington, DC, USA. Piscataway: IEEE Press, 2016.
- [12] WANG X, LIU Z, LI J, et al. Tualatin: towards network security service provision in cloud datacenters[C]//2014 3rd International Conference on Computer Communication and Networks, August 4-7, 2014, Shanghai, China. Piscataway: IEEE Press, 2016.
- [13] LOPEZ D, LOPEZ E, DUNBAR L, et al. Framework for interface to network security functions. Internet-Draft draft-ietf-i2nsf-framework-08, IETF Secretariat, October 2017[R/OL]. (2017-10-10)[2017-11-10]. <https://www.ietf.org/archive/id/draft-ietf-i2nsf-framework-08.txt>.
- [14] OpenDaylight SFC project [EB/OL]. (2016-10-21)[2017-11-10]. <https://github.com/opendaylight/sfc>.
- [15] Docker [EB/OL]. (2017-01-01)[2017-11-10]. <https://www.docker.com>.
- [16] Open vSwitch [EB/OL]. (2016-01-01)[2017-11-10]. <http://openvswitch.org>.
- [17] Redis [EB/OL]. (2017-01-01)[2017-11-10]. <https://redis.io>.
- [18] Openstack [EB/OL]. (2017-01-01)[2017-11-10]. <https://www.openstack.org>.
- [19] Iptables [EB/OL]. (2014-01-01)[2017-11-10]. <http://www.netfilter.org/projects/iptables/index.html>.

- org/projects/iptables/index.html.
- [20] Snort [EB/OL]. (2017-01-01)[2017-11-10]. <https://www.snort.org>.
- [21] PAUL Q, URI E, CARLOS P. Network service header (NSH): Internet-Draft draft-ietf-sfc-nsh-28[EB/OL]. (2017-11-03)[2017-11-10]. <http://www.ietf.org/internet-drafts/draft-ietf-sfc-nsh-28.txt>.
- [22] Conf D[EB/OL]. (2017-01-01)[2017-11-10]. <http://developer.cisco.com/site/confd>.

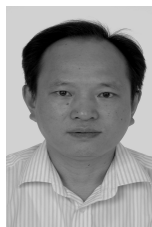
[作者简介]



胡腾(1988-), 男, 中国工程物理研究院计算机应用研究所工程师, 主要研究方向为计算机技术与信息安全。



李观文(1992-), 男, 北京交通大学电子信息工程学院博士生, 主要研究方向为软件定义网络与网络安全。



周华春(1965-), 男, 博士, 北京交通大学电子信息工程学院教授、博士生导师, 主要研究方向为移动互联网、网络安全与卫星网络。