# 面向云化网络的资产安全管理方案

## Asset Security Management Solution for Cloud Network

张小梅[1]，袁苏文[2]，马　铮[1]，张曼君[1]，高　枫[1]（1. 中国联通网络技术研究院，北京 100048；2. 中国电子科技集团公司电子科学研究院，北京 100041）

Zhang Xiaomei[1], Yuan Suwen[2], Ma Zheng[1], Zhang Manjun[1], Gao Feng[1]（1. China Unicom Network Technology Research Institute, Beijing 100048, China; 2. China Academy of Electronic Sciences, Beijing 100041, China）

**摘　要：**

随着虚拟化技术的推进，整个电信网正向着自定义、虚拟化、智能化方向不断演进，安全性问题逐渐成为制约网络发展的关键因素。分析当前云网络资产管控面临的安全问题，结合资产自发现、指纹识别、信息安全管理技术，介绍了一种基于SDN/NFV技术的资产安全管理方案，实现云网络安全能力重构，该方案具有安全服务快速部署、安全资源灵活调度等特点，可实现资产安全信息动态更新与精确管理。

**关键词：**

SDN；NFV；虚拟化

**doi：**10.12045/j.issn.1007-3043.2019.04.003

**中图分类号：**TN929.5

**文献标识码：**A

**文章编号：**1007-3043（2019）04-0012-04

**Abstract：**

With the advancement of virtualization technology, the telecommunication network is evolving towards customization, virtualization and intellectualization. Security has gradually become a key factor restricting the development of network. It analyzes the current security problems faced by cloud network asset management. Combined with asset self-discovery, fingerprint identification and information security management technology, it introduces an asset security management scheme based on SDN/NFV technology to realize cloud network security capability reconstruction. The solution has the characteristics of rapid business deployment and flexible resource scheduling, and realizes dynamic updating and precise management of asset security information.

**Keywords：**

SDN; NFV; Virtualization

**引用格式：**张小梅，袁苏文，马铮，等. 面向云化网络的资产安全管理方案[J]. 邮电设计技术，2019(4)：12-15.

## 0 前言

随着互联网的快速发展，电信运营商的业务发生了重大变革，为此寻找更灵活、更高效、低成本的网络架构解决方案成为运营商关注的焦点。云化网络作为一种新型的网络架构，其倡导的虚拟化能全面突破现有网络困境。在云化网络架构下，原来的硬件网元设备的物理边界消失，引入更多软件安全问题，攻击面变得更广，云化网络的资产安全管理显得越来越重要。尽管现在安全风险排查力度不断加大，但尚未完全掌握在网全量资产安全信息，安全巡检的盲点仍然很多，大量安全漏洞一直潜伏在系统中，查找定位问题源头较为困难。如何对云化网络的基础资源、虚拟网元进行安全调度和管理，成为业界普遍面临的重要问题，SDN/NFV作为下一代网络变革的核心技术，具有集中控制、资源灵活调度等特性，易于实现统一安全管控及安全能力重构。本文基于SDN/NFV技术设计了自动化、智能化的云化网络资产安全管理解决方案，实现网络资产安全信息动态更新和精确管理。

**收稿日期：**2019-02-19

## 1 云化网络架构

云计算促使传统硬件资源从无共享、系统封闭、运维流程复杂的网络向资源虚拟化的按需分配的云网络转型，云化网络中采用虚拟化技术对各种资源进行虚拟化，打破了传统电信设备竖井式体系，所有的业务都可以通过MANO分配虚拟化资源、实例化VNF等实现新业务快速部署、资源灵活调度，简化运维、提高网络资源利用率。图1显示了云化网络架构，从功能上来划分，可以分为MANO管理与协同模块、虚拟化的网络实体层、网络虚拟化功能基础设施层。

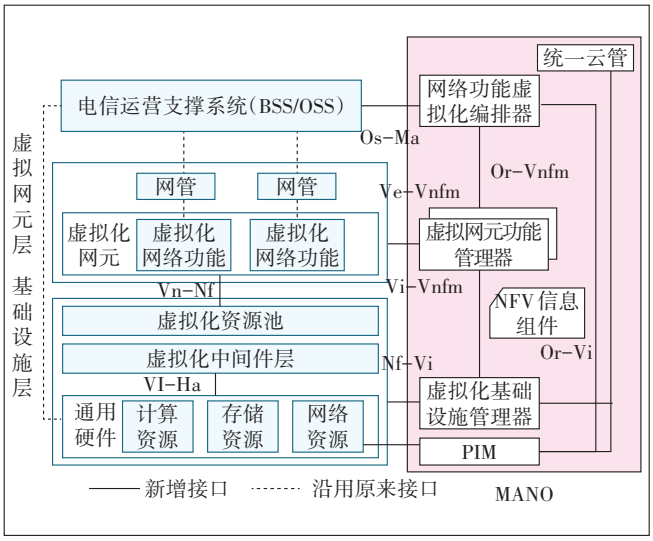


图1　云化网络架构

a）MANO管理与协同模块：负责虚拟机生命周期管理、资源监控、虚拟机性能监控、故障管理、虚拟机动态迁移、资源管理、信息维护等。

b）虚拟化的网络实体层：实现传统网络功能虚拟化，以软件的形式运行在虚拟机上。

c）网络虚拟化功能基础设施层：包括各种物理硬件资源、虚拟资源及Hypervisor，是支持VNF运行的环境。

## 2 资产安全管控关键技术

### 2.1 资产存活性探测

资产存活性探测用于探测网络中资产的在线情况，资产存活性探测可采用登录采集方式和远程扫描探测方式，可以根据不同的网络环境灵活选择资产发现方式，摸清企业资产存活情况，从而掌握企业全网资产上下线情况。

登录采集方式：通过登录业务系统的网络采集路由/交换设备相关配置信息，激活所有在网设备，根据获取的ARP表、MAC表、路由表、接口信息表等信息汇总形成完整资产列表，实现在网资产的全量发现。

扫描探测方式：通过发送探测包到指定IP，根据回复情况来判断资产存活情况，发送的探测包可以是ARP、ICMP、TCP SYN/ACK包、UDP、SCTP等。

a）ARP协议探测：通过向目标资产发送ARP Request包，在探测包超时前如果接收到目标资产的ARP Re-sponse包，则此资产存活。

b）ICMP协议探测：通过向目标资产发送ICMP请求包，根据应答报文的类型判断资产的活跃状态。

c）TCP SYN/ACK协议探测：通过向目标资产发送TCPSYN/ACK探测包，在探测包超时前如果收到目标资产的TCP应答报文是RST包或SYN/ACK包，则此资产存活。

d）UDP协议探测：通过向目标资产发送UDP探测包，在探测包超时前如果收到目标资产的UDP应答报文，则此资产存活。

e）SCTP协议探测：通过向目标资产发送SCTP INIT探测包，在探测包超时前如果收到目标资产的SCTP应答报文，则此资产存活。

### 2.2 资产指纹信息识别

在资产存活性探测的基础上，对存活资产进行指纹信息收集，首先需要确定资产端口开放情况，以及端口上运行的具体应用程序与版本信息，然后进行操作系统的侦测，最后对资产安全基线配置、漏洞等信息进行收集，指纹信息主要包括以下几种。

a）开放端口：资产对外开放的端口信息。

b）软件版本：资产上运行的软件版本信息。

c）操作系统：资产的操作系统类型及版本信息。

d）安全基线配置：资产配置信息，用于核查是否存在不合规的配置。

e）网站漏洞：网站漏洞信息，并检测弱密码和撞库攻击。

f）系统漏洞：资产系统漏洞信息，用于发现潜在的漏洞隐患。

资产指纹采集方式主要包括远程探测和登录获取2种方式，远程探测方式是通过发送数据包去主动探测网络资产，通过返回的报文信息来识别资产指纹信息。登录获取方式是通过与网络中的4A系统（集账号管理、授权管理、认证管理、审计管理功能于一体的身份识别与访问管理系统）进行对接，通过4A系统的指令通道来获取指纹信息。针对未知资产可以采用远程探测方式，已纳入4A系统管控的资产可以利用指令通道直接获取资产指纹信息。

a）远程探测方式：通过发送探测包到指定IP，根据回复情况来判断资产指纹信息情况，发送的探测包可以是TCP、ICMP、UDP等。

b）登录获取方式：对于已经纳入4A系统管控的资产，可利用4A系统指令通道接口来获取资产指纹信息，4A系统指令通道接口是指为各类维护或管理平台、维护人员自行开发的自动化程序提供的程序调用接口，可以解决自动化程序通过4A系统访问接入资源

的问题。因此，只需要编制指纹信息获取的自动化脚本程序，即可通过指令通道提取出资产的指纹信息。

图2示出的是登录获取方式流程。

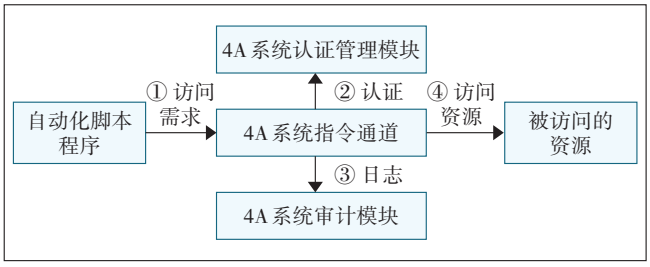


图2　登录获取方式流程

### 2.3 资产安全信息管理

目前网络中存在退网资产仍在线运行、未经管理流程违规上线、擅自更改资产用途、携带各类安全问题等情况，这将成为企业网安全短板，是恶意入侵利用的主要目标。精确的资产安全信息管控是信息安全的基础，因此，需要对资产安全信息进行全生命周期管理，定位存在安全隐患的系统或组件。

资产安全信息管理主要包括存活性和安全指纹信息管理，根据网络业务具体需求，对指定扫描范围的所有IP地址进行周期性存活探测，发现存活资产，进而对已存活的资产进行指纹信息获取，并将获取的资产指纹信息与历史资产快照进行对比，查看资产指纹信息是否有变更，并全面分析资产存在的安全基线、漏洞等问题。

图3示出的是资产异常管理。

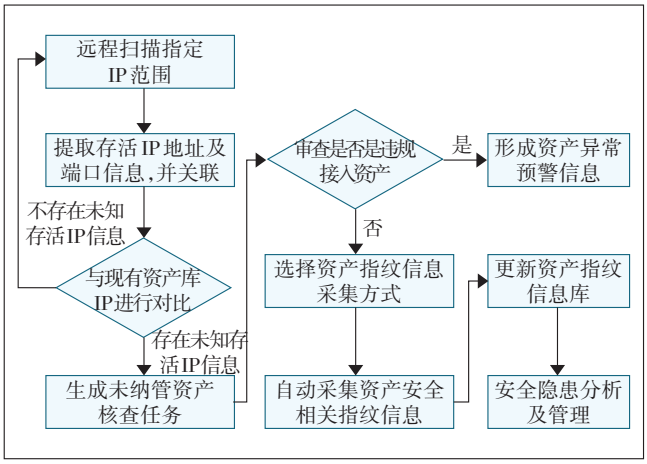


图3　资产异常管理

a）通过远程扫描方式周期性探测资产库里面设备的存活状态，如果发现设备不在线，则核对设备是否已下线，确认下线就更新资产库信息，确认不是正常下线就展示资产异常告警；如果发现设备存活，则获取资产指纹信息。

b）将获取的资产指纹信息与历史资产快照进行对比，查看资产指纹信息是否有变更，如果无变更，则继续周期性探测资产库设备存活状态；如果有信息变更，则对变更的信息进行分析，分析是否存在安全隐患，并对存在的安全隐患进行全生命周期闭环管理。

## 3 云化网络资产安全管理方案

### 3.1 云化网络资产安全管理系统架构

借助SDN/NFV网络控制与转发平面分离、集中控制、开放可编程等特性，设计了云化网络资产安全管控系统架构（见图4），实现统一安全管控及安全能力重构。通过安全资源虚拟化技术对网络中的安全能力进行抽象，形成满足特定安全需求的安全虚拟机，再由安全编排和控制器对安全策略、安全功能和网络流量进行动态的编排，实现可重构安全资源的按需部署和动态伸缩的同时，为企业内部及客户提供满足其需求的资产安全评估服务。

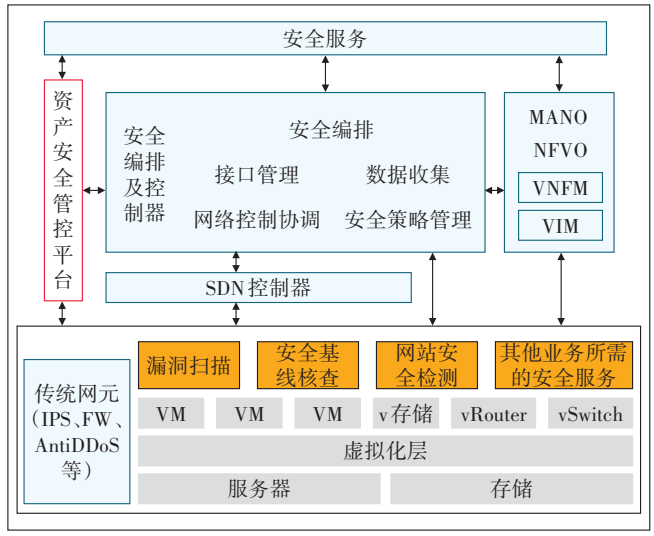


图4　云化网络资产安全管理系统架构

a）安全服务：安全业务服务模块是整个系统的核心，负责处理系统的安全业务逻辑。

b）安全编排及控制器：负责对安全设备策略、安全功能和网络流量进行动态的管理和编排，并通过监控网络设备及安全设备运行状态，实现对相关安全数据的采集。

c）资产安全管控平台：负责对采集资产指纹信息及日志信息进行关联分析，并对发现的安全问题进行全生命周期闭环管理。在安全分析过程中，如发现异

常情况将进行预警，并通知安全编排及控制器调整安全策略。

d）SDN控制器：根据业务需求，负责各厂家网络或逻辑域内网络的路由、QoS等策略生成与下发。

e）MANO：实现对安全资源的管理，虚拟化安全网元的生命周期管理及初始化配置。

f）安全资源池：包含安全设备以及交换机、路由器等网络设备。

### 3.2 云化网络资产安全评估服务运营流程

以漏洞扫描服务为例，对云化网络资源漏洞清点及问题跟踪进行详细解析，具体运营流程如图5所示。

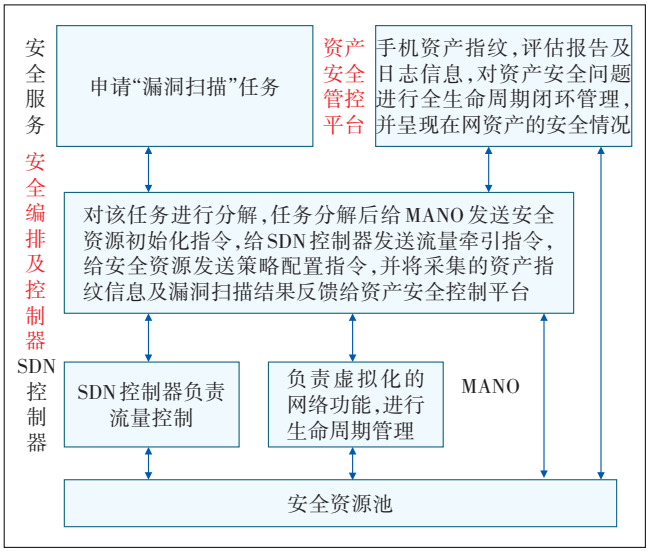


图5　漏洞扫描服务运营流程

a）申请网络资产所需的漏洞扫描服务，并将漏洞扫描服务任务下发给安全编排及控制器。

b）安全编排及控制器根据需要进行漏洞扫描的资产范围，确定漏洞扫描服务路径经过的所有节点，将流量调度策略下发给SDN控制器，将漏扫设备配置策略下发给MANO。

c）漏洞扫描服务路径经过的所有节点由控制器下发SDN流表，构建安全服务链，由MANO对漏扫设备进行初始化，并由安全编排及控制器对其进行安全策略配置。

d）进行漏洞扫描服务，并将执行结果和日志信息反馈给资产安全管控平台，由资产安全管控平台进行关联分析及呈现，必要时须对安全方案进行调整。

## 4 结束语

借鉴现有信息系统安全模型由安全策略、防护、检测和响应共同构成完整安全体系的思想，并把安全能力池作为功能基础，将安全能力构建过程设计为动态可调整过程，并在此过程中融合了业务安全需求分析、安全方案适配、安全服务链构建、安全服务动态调整、网络资产安全态势分析等机制，以实现基于SDN/NFV技术的资产安全管控解决方案，以保证云化网络在引入虚拟化技术后的资产安全，保证新网络能力和业务能够在安全的资产上运行。

**参考文献：**

[1] 沈庆国，张高明，骆坚. SDN特征剖析及典型应用介绍[J]. 移动通信，2014(14).
[2] 张朝昆，崔勇. 软件定义网络(SDN)研究进展[J]. 软件学报，2015，26(1)：62-81.
[3] 左青云. 基于OpenFlow的SDN技术研究[J]. 软件学报，2013，24(5)：1078-1097.
[4] 龚向阳，王文东. 一种面向多样化网络业务融合的SDN网络架构[J]. 中兴通讯技术，2013，19(5)：16-21.
[5] 张小梅. 云数据中心安全防护解决方案[J]. 邮电设计技术，2016(1)：50-54.
[6] 刘文懋，裘晓峰，陈鹏程，等. 面向SDN环境的软件定义安全架构[J]. 计算机科学与探索，2015，9(1)：63-70.
[7] 王淑玲，李济汉，张云勇. SDN架构及安全性研究[J]. 电信科学，2013，29(3)：117-122.
[8] 李军，王翔. 云数据中心网络安全的新挑战[J]. 保密科学技术，2013(8)：6-11.
[9] 肖贵福. 基于虚拟化安全网络扩展的SDN安全架构[J]. 现代计算机(专业版)，2014(21)：6-10.
[10] 周向军. 云计算数据中心的安全体系架构设计[J]. 江苏理工学院学报，2015(2)：27-34.
[11] 肖小兵. 云计算数据中心网络安全的实现原理探析[J]. 无线互联科技，2013(6)：22-23.
[12] 王军. 云计算系统资源调度及安全性研究[D]. 武汉：武汉理工大学，2013.
[13] 张新涛，周君平，杜佳颖，等. 云数据中心的安全虚拟网络[J]. 信息安全与通信保密，2012(11)：85-88.
[14] 赵雷霆. 运营商级云计算数据中心发展研究[J]. 网络空间安全，2011(8)：36-39.
[15] 张旭辉. 运营商云数据中心网络安全技术研究综述[J]. 中国新通信，2015(9)：19-20.
[16] 李知杰. 云计算数据中心网络安全的实现原理[J]. 软件导刊，2011(2)：123-125.

**作者简介：**
张小梅，工程师，硕士，主要研究方向为网络安全相关领域；袁苏文，主要从事通信领域的研究工作；马铮，高级工程师，博士，主要研究方向为网络安全相关领域；高枫，高级工程师，博士，主要研究方向为网络安全相关领域；张曼君，高级工程师，博士，主要研究方向为网络安全相关领域。