计算机系统应用 ISSN 1003-3254, CODEN CSAOBN
Computer Systems & Applications,2018,27(8):81−86 [doi: 10.15888/j.cnki.csa.006506]

E-mail: csa@iscas.ac.cn
http://www.c-s-a.org.cn
Tel: +86-10-62661041

# 面向健康云的定制化网络安全服务①

陈雅琳[1,2], 刘　薇[2,3], 徐　安[1,2], 李巧平[2,5], 何　进[1], 陈雷霆[1,4,5]

[1](电子科技大学 计算机科学与工程学院, 成都 611731)
[2](东莞迪赛软件技术有限公司, 东莞 523808)
[3](成都工业职业技术学院, 成都 610218)
[4](电子科技大学 广东电子信息工程研究院, 东莞 523808)
[5](广东省卫生厅政务服务中心, 广州 510060))
通讯作者: 陈雷霆, E-mail: richardchen@uestc.edu.cn

**摘　要**: 针对传统的云计算网络安全模式无法满足云用户不同的网络安全需求, 本文提出一种面向健康云的定制化网络安全服务方案. 该方案首先根据健康云用户的网络安全需求填写安全模板; 然后, 将安全模板进行加密; 最后, 由定制化网络安全服务系统自动分析处理, 建立有效的安全规则, 最终保护云用户安全. 在医疗健康云平台上展开实验, 对比传统方法, 实验结果显示本文方法在性能改善上的有效性.

**关键词**: 健康云; 网络安全; 定制化; 安全模板

引用格式: 陈雅琳,刘薇,徐安,李巧平,何进,陈雷霆.面向健康云的定制化网络安全服务.计算机系统应用,2018,27(8):81–86. http://www.c-s-a.org.cn/1003-3254/6506.html

## Customized Network Security Service for Health Cloud

CHEN Ya-Lin[1,2], LIU Wei[2,3], XU An[1,2], LI Qiao-Ping[2,5], HE Jin[1], CHEN Lei-Ting[1,4,5]

[1](Computer Science and Engineering Academy, University of Electronic Science and Technology of China, Chengdu 611731, China)
[2](Dongguan Data Science Software Technology Co. Ltd., Dongguan 523808, China)
[3](Chengdu Vocational and Technical College of Industry, Chengdu 610218, China)
[4](Institute of Electronic and Information Engineering in Dongguan, University of Electronic Science and Technology of China, Dongguan 523808, China)
[5](Government Affairs Service Center of Guangdong Provincial Health Department, Guangzhou 510060, China)

**Abstract**: In view of the traditional cloud computing network security model can not satisfy the different network security needs of cloud users, this study proposes a customized network security service solution for health cloud. This scheme firstly fills in the security spec according to the health cloud user's network security requirements. Then, encrypt the security spec. Finally, the customized network security service system automatically analyzes and processes to establish effective security rules and ultimately protect the cloud user security in the medical health cloud platform. Compared with the traditional method, the results show that the proposed method is effective in improving performance.

**Key words**: health cloud; network security; customization; security spec

基于云模式的健康服务是居民健康服务发展的必然趋势. 这种服务模式增加了数据和业务的共享利用, 同时节约了成本, 但也引入了新的安全威胁, 这些年来受到越来越多的关注和研究. 除了隐私安全保护[1,2], 云计算中的网络安全威胁也是重要研究方向, 如云平台自身的安全[3]、底层虚拟资源和系统的安全[4]、云服

① 基金项目: 国家 863 计划 (2015AA016010); 广东省应用型科技研发专项基金 (2015B010131002); 东莞市重大科技项目 (2015215102)
Foundation item: National High-tech R & D Program of China (863 Program) (2015AA016010); Special Project for Applied Research of Guangdong Province (2015B010131002); Key Project of Dongguan (2015215102)
收稿时间: 2017-11-27; 修改时间: 2018-01-31; 采用时间: 2018-02-06; csa 在线出版时间: 2018-07-28

务商不可信[5]、链路攻击导致用户敏感信息的泄露[6]、共享安全漏洞等[7,8]等。

## 1 传统网络服务安全面临的挑战

近年来, 这些问题得到了研究者们的大量关注[9–12], 然而, 在传统的云计算网络安全模式中, 由于云服务商对云用户的服务安全需求不了解, 无法按需提供安全服务, 如图 1 所示. 云计算提供成千上万种类型的服务, 即使相同类型的服务, 其安全需求也有差异. 传统的云模式缺乏自动安全规则配置[13,14], 服务商无法掌握每类服务的安全需求, 只能根据用户需求针对每个服务进行手工配置, 后期进行人工维护和管理, 这是几乎不可能完成的任务, 使得居民健康服务平台无法得到可信可控的云安全服务, 最终导致居民、医院医疗机构、政府卫生机构及第三方相关机构的网络安全仍面临很大的网络安全威胁. 针对这个问题, 本文结合文献[15]的思想, 提出一种定制化的健康云网络安全服务方案.

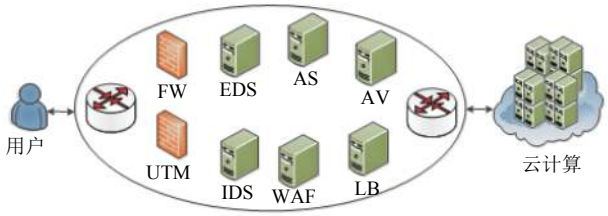


图 1 传统的云计算网络安全模式

## 2 面向健康云的定制化网络安全

### 2.1 面向健康云的定制化设计思想及架构

健康云的用户主要有居民、医院医疗机构、政府卫生机构以及第三方机构等. 健康云应用如图 2 所示, 在健康云上实现移动终端和健康档案管理系统之间的数据传输服务; 健康档案管理, 包括健康档案查询服务、预约挂号服务、健康知识推送服务、居家健康服务、健康咨询服务、大数据智能分析等.

面向健康云的网络安全定制化服务主要由 5 个部件组成: SMG, SMD, Dom0, 服务域 (service domains), 虚拟交换机 (vSwitch). 为了保证服务域的网络安全, 无论何时访问服务域, 外部流量或内部流量需要通过所需的过滤域; 若网络受到攻击, 则将攻击日志存放在日志管理域 (ELMD) 中, 如图 3 所示.

SMG 由反垃圾邮件 (AS) 组, 防火墙 (FW) 组, 防病毒 (AV) 组等安全组构成, 负责将检测和过滤产生的攻击日志和统计信息等保存到 SMD 中的事件和 ELMD 里.

SMD 主要由管理域 (MD) 和 ELMD 组成. 其中, ELMD 存储和管理来源于 SMG 的事件和日志. MD 主要负责的功能为: 创建/删除 SMG 中的任何域; 下发转发规则到 vSwitch, 让访问服务域流通过对应的安全检测链路 (FMC), 进行安全检测过滤; 收集 SMG 中每一个组的状态信息 (如负载, 失效) 和接受来自 vSwitch 的转发信息 (如流量).

Dom0 缩减了权限, 不能创建/启动和停止/删除 SMG 中的任何域 (domain), 但仍然保持权限去处理并管理服务器域中任何虚拟机, 包括按照时间片进行调度、I/O 分配等.

Service domains 承载多类型的基于网络的健康云用户服务, 如 FTP 服务, Web 服务等.

vSwtich 负责接受 MD 下发的转发规则, 并且转发内外流通过安全域进行检测和过滤.

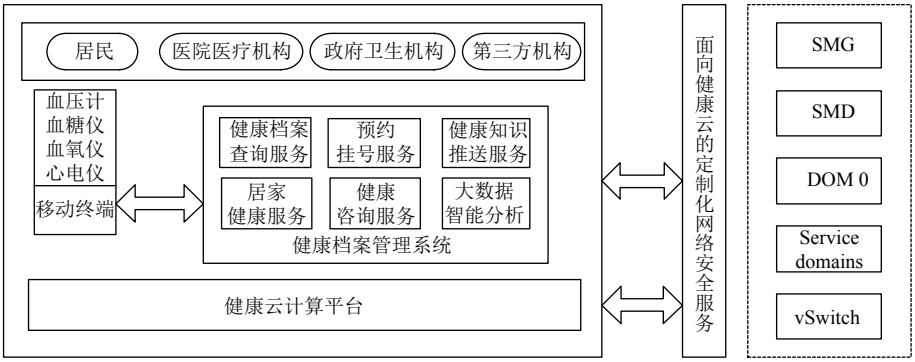


图 2 面向健康云的定制化网络安全服务应用

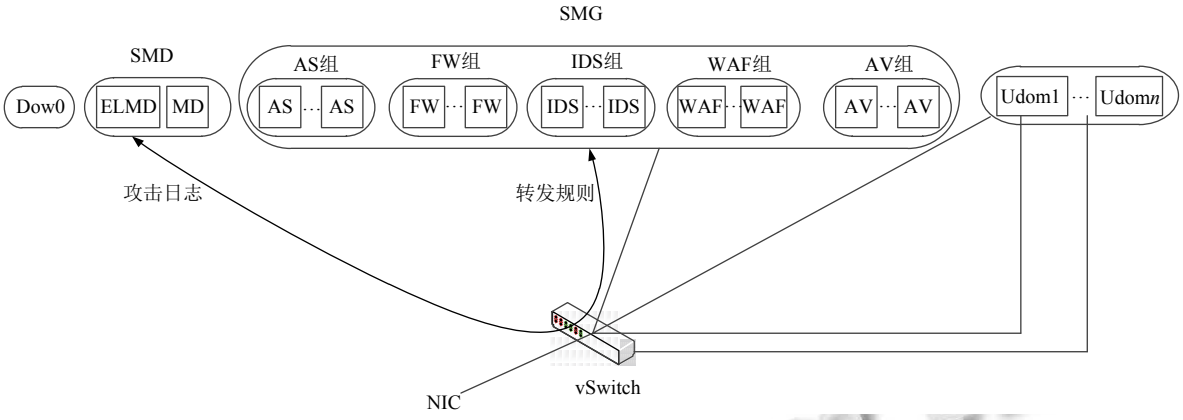


图 3 面向健康云的网络安全定制化服务应用

MD 主要由 SPEC 分析器和 RouteGen 转化器组成. SPEC 分析器通过云用户 SPEC、网络设备(Mbox) 状态信息、Mbox 拓扑和 vSwitch 信息进行分析, 生成 FMC 安全路径和安全过滤规则. RouteGen 转化器将 FMC 安全路径转化为转发规则, 通过转发流到 FMC 链进行安全检测和过滤. 最终 MD 将转发规则下发到 vSwitch 中, 将安全过滤规则转发到对应的 Mbox 中.

为了便于虚拟 Mbox 日志的识别和标准化管理, 虚拟 Mbox 应该具备统一日志格式. 包括: 日志类型、Mbox 唯一标识、事件标示、某个特定服务唯一标示、源 IP、源端口、目的 IP、目的端口、Protocol 以及日志事件的详细描述. 当 ELMD 接受日志后, ELMD 的日志分类器将这些日志进行分类便于基于用户权限访问. 面向健康云的定制化网络安全整体设计如图 4 所示.

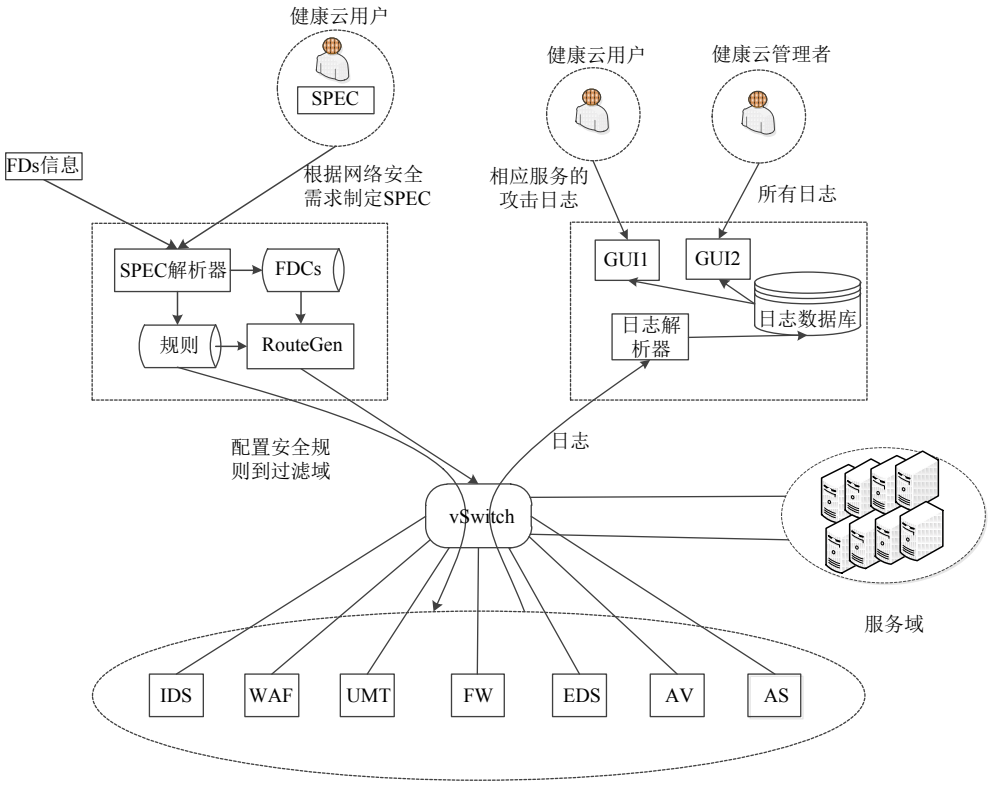


图 4 面向健康云的定制化网络安全服务总体设计

针对健康云的网络安全服务要求, 定制化安全分析算法伪代码如下:

算法 1. 定制化安全分析算法

1) 根据不同角色的健康云用户的网络安全需求填写提供的 SPEC.
2) 对 SPEC 进行加密并提交给 CNS.
3) MD 根据 SPEC, 自动生成 FMC 及其路径上对应的安全规则, 分别下发到 vSwitch 和对应 Mbox 中, 对访问流进行检测和过滤.
4) CNS 将 Mbox 生成的日志发送给 ELMD, 经分析后处理后, 存放在日志数据库中.
5) ELMD 根据角色权限的不同, 分别为云服务商管理者和健康云用户提供不同的 GUI 管理界面, 不同角色的用户拥有不同的查询权限, 例如健康云用户只能查询自己相关服务的攻击日志, 而管理者可查询所有的攻击日志.

### 2.2 定制化网络安全实现算法

SPEC 安全模板的主要参数包括需要保护的 IP 和端口; 网络层、AV、AS、Web 检查和安全传输, 每一项都对应相应的虚拟 Mbox; 网络层和安全检查, 其结构如图 5 所示.

CNS 系统对接收到的加密安全模板 SPEC 首先进行解密并分析它, 自动分析过程实现算法伪代码如下:

算法 2. SPEC 自动分析算法

输入: SPEC 模板.
输出: 安全规则集合.

1) 提取 IP 和端口对, 获取一组云用户服务.
2) 初始化所有被保护对象的 FMC 和安全规则, 初始值置为空.
3) 根据被保护对象的 SPEC 中的 yes 项配置安全规则到对应的虚拟 Mbox 中.
4) 如果所有被保护对象的安全规则配置完, 转第 5) 步; 否则转到第 3) 步.
5) 添加为被保护对象提供网络安全服务的虚拟 Mbox 到 FMC 中.
6) 如果所有被保护对象的虚拟 Mbox 都添加到 FMC 中, 算法结束; 否则, 转到第 4) 步.

上述算法不但可以检测出光流扰动效应, 还可以判断是否检测到运动目标, 如果判断为检测到了运动目标, 就发出提示信息并且把当前帧图像保存下来, 如果仅仅检测光流扰动效应, 则可以把该算法简化, 省略第 4) 步.

## 3 仿真实验

### 3.1 实验环境与评价指标

本实验采用 6 核超线程 2.8 GHz Intel 处理器、16 G 内存 DELL 服务器作为云计算硬件服务器; IXIA 和 iperf 作为性能测试工具; 使用 3.4.2 版本的 XEN Hypervisor, 内核为 2.6.31 的 Fedora16 系统的 Dom0; 使用 2.6.27 内核 64 位 Fedora 系统作为虚拟客户机, vSwitch 带宽为 1 G 网络; 安全软件使用开源的 IPFire、ModSecurity、OpenSSL、PacketFence 作为实验软件.

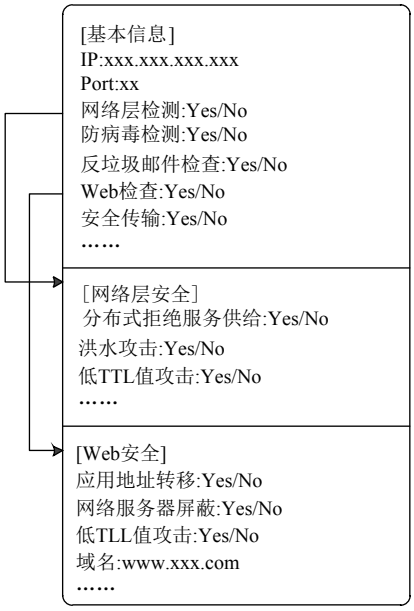


图 5 面向健康云的定制化网络用户安全模板

实验以网络延迟、网络吞吐量、丢包率三个性能参数作为评价指标进行分析, 以 Web 服务为例, 检测该系统面对攻击的防护能力.

### 3.2 实验结果与分析

本文对 3 种安全服务算法 (UTM、CNS-unbind-core、CNS-bind-core) 的网络安全系统性能进行实验对比. 实验基于 UDP 的数据包转发和基于 TCP 的网络访问两种服务类型对 3 种算法相对于无网络安全服务情况的网络延迟、吞吐量、以及丢包率的增大或减小程度进行对比, 延迟和丢包率增大的程度越低且吞吐量减少的程度越低, 说明性能越好.

第一组实验对比 UTM 和 CNS-unbind-core 的系统性能, 以此说明本文所提方法的有效性. CNS-unbind-core 是使用本文所提出的 CNS 方法, 与 UTM 将所有安全软件移植到一个 VM 中不同, 它是将每个安全软件放在不同的 VM 中, 由多核系统自由调度. 表 1、2、3 显示了 UDP 在 3 种算法下相对无网络安全服务的网络延迟增大程度、吞吐量减小程度以及丢包率的增大程度比较. 表 1 的第一和、二行表明 UTM 相对于 CNS-unbind-core 的平均延迟增加了 0.8%; 表 2 的第一、二行表明 UTM 相对于 CNS-unbind-core 平

均吞吐量减少了 0.9%; 表 3 的第一、二行表明 UTM 相对于 CNS-unbind-core 平均丢包率增加了 0.8%. 基于 TCP 的网络访问, 除了数据包大小从 1024 bit 到 65 536 bit 之外, 实验方法类似于 UDP 转发. 表 4、5、6 显示了基于 TCP 的网络访问在三种算法下相对无网络安全服务的网络延迟增大程度、吞吐量减小程度以及丢包率的增大程度比较. 表 4 的第一、二行表明 CNS-unbind-core 相对于 UTM 的平均延迟降低了 42.3%; 表 5 的第一、二行表明 CNS-unbind-core 相对于 UTM 的平均吞吐量增加了 6.4%; 表 6 的第一、二行表明 CNS-unbind-core 相对于 UTM 的平均丢包率降低了 6.4%. 实验数据表明, TCP 数据包大小与性能之间的关系类似于 UDP 转发, 但 CNS-unbind-core 的三个性能指标都高于 UTM, 尤其是大幅度降低了平均延迟. 无论是 UDP 转发, 还是基于 TCP 的网络访问, CNS-unbind-core 实现的系统性能都高于 UTM. 因此, 采用 CNS-unbind-core 而不是 UTM, 可以实现更好的系统性能.

表 1 UDP 在三种算法下的网络延迟增大程度比较 (%)

| 数据包大小 (bites) | 64 | 128 | 256 | 512 | 1024 | 1280 | 1518 |
|---|---|---|---|---|---|---|---|
| UTM | 40 | 17.3 | 37.5 | 23 | 16 | 35.7 | 23.5 |
| CNS-unbind-core | 40 | 17.3 | 37.5 | 21 | 17.4 | 32.9 | 21.8 |
| CNS-bind-core | 8 | 4.4 | 4.8 | 7.9 | 4.3 | 8.6 | 11.8 |

表 2 UDP 在三种算法下的网络吞吐量减少程度比较 (%)

| 数据包大 (bites) | 64 | 128 | 256 | 512 | 1024 | 1280 | 1518 |
|---|---|---|---|---|---|---|---|
| UTM | 19.4 | 12.2 | 9.1 | 11.3 | 12.5 | 0 | 0 |
| CNS-unbind-core | 16.1 | 9.8 | 9.1 | 7.5 | 15.3 | 0 | 0 |
| CNS-bind-core | 9.7 | 4.9 | 4.5 | 3.8 | 12.5 | 0 | 0 |

表 3 UDP 在三种算法下的丢包率增大程度比较 (%)

| 数据包大小 (bites) | 64 | 128 | 256 | 512 | 1024 | 1280 | 1518 |
|---|---|---|---|---|---|---|---|
| UTM | 6 | 2.4 | 0.5 | 0 | 0 | 0 | 0 |
| CNS-unbind-core | 6 | 2 | 0.7 | 0 | 0 | 0 | 0 |
| CNS-bind-core | 0 | 0 | 0 | 0 | 0 | 0 | 0 |

由 UTM 和 CNS-unbind-core 基于 TCP 的网络访问这组对比实验可以得出, UTM 的上下文切换和争用单个虚拟机上的共享资源 (尤其是 CPU 资源) 带统开销高于 CNS-unbind-core 中 VM 间通信和缓存无效带来的系统开销. 如果在多核虚拟平台上使用 CNS 执行并行检查, 则可以克服资源争用竞争, 能显着提高系统性能.

第二组实验对比了 CNS-unbind-core 与 CNS-bind-core 的系统性能, CNS-bind-core 在 CNS-unbind-core 的基础上将每个 VM 绑定一个 core. 表 1 至表 6 的第二、三行实验数据表明, CNS-bind-core 在 UDP 转发和网络访问的延迟、吞吐量和丢包率上明显优于 CNS-unbind-core. 在绑定多核时, 定制化网络安全服务充分利用系统资源是有利因素, 克服了单个虚拟机上共享资源的上下文切换; 但是增加了 interVM 之间的通信开销, 并导致 VM 间切换之间的缓存无效. CNS-bind-core 可以充分利用硬件辅助的 I/O 虚拟化技术; 另外, 多核调度不断地在多个 VM 之间切换, 导致相应的缓存无效, 从而导致系统性能下降. 每个 FD 被绑定到 CPU 内核以克服缓存无效, 从而克服了缓存无效的缺点.

表 4 TCP 在三种算法下的网络延迟增大程度比较 (%)

| 数据包大小 (bites) | 64 | 128 | 256 | 512 | 1024 | 1280 | 1518 |
|---|---|---|---|---|---|---|---|
| UTM | 70 | 57.1 | 90 | 45.1 | 85 | 69.8 | 78.6 |
| CNS-unbind-core | 50 | 28.6 | 10 | 19.4 | 25 | 26.4 | 40 |
| CNS-bind-core | 0 | 0 | 0 | 3.2 | 5 | 9.4 | 14.3 |

表 5 TCP 在三种算法下的网络吞吐量减少程度比较 (%)

| 数据包大 (bites) | 64 | 128 | 256 | 512 | 1024 | 1280 | 1518 |
|---|---|---|---|---|---|---|---|
| UTM | 20.8 | 25.7 | 20.9 | 0 | 0 | 0 | 0 |
| CNS-unbind-core | 8.3 | 10.9 | 3.1 | 0 | 0 | 0 | 0 |
| CNS-bind-core | 5.6 | 6.3 | 0 | 0 | 0 | 0 | 0 |

表 6 TCP 在三种算法下的丢包率增大程度比较 (%)

| 数据包大小 (bites) | 64 | 128 | 256 | 512 | 1024 | 1280 | 1518 |
|---|---|---|---|---|---|---|---|
| UTM | 8 | 5.4 | 2.5 | 0.2 | 0 | 0 | 0 |
| CNS-unbind-core | 6.4 | 3.8 | 1.3 | 0 | 0 | 0 | 0 |
| CNS-bind-core | 6 | 2.8 | 0.3 | 0 | 0 | 0 | 0 |

第三组实验对比了在健康云中使用 CNS-bind-core 保护网络安全和不采取任何措施保护健康云的网络安全的系统性能. 表 1 至表 6 的第三行实验数据表明, 不采用任何措施保护网络安全相比于 CNS-bind-core 而言, 表现出更好的系统性能, 但是如果不采取保护措施来保护云计算安全性, 可能导致无法估量的损失. 因此, 只要采用保护措施的性能开销在可接受范围内即可. 仍然用 UDP 转发、网络访问两组实验来评估 CNS-bind-core 的性能影响.

对于 UDP 转发, 表 1、表 2、表 3 的第三行实验数据显示, 在健康云中使用 CNS 比没有使用网络安全服务的平均延迟增加了 7.11%, 平均吞吐量下降 5.1%. 丢包率受到安全检查和过滤的影响, 这些性能开销是不可避免的检查和过滤 UDP 流量. 由于 UDP 流量必须经过 FW 检测和过滤, 才能转发到服务域中的 UDP 服务器. 在此过程中, 流量需要匹配 FW 中数百个过滤规则, 导致延迟增加和吞吐量下降. 与 UTM 相比, CNS-bind-core 的性能已经有了很大的提升.

基于 TCP 的网络访问, 在健康云中使用 CNS-bind-core 与无网络安全服务情况比较, 延迟受影响较大, 吞吐量几乎不受影响. 表 4、表 5、表 6 的第三行实验数据进一步说明, 使用 CNS-bind-core 保证健康云网络安全后平均延迟增加 4.6%, 平均吞吐量下降 1.7%, 平均丢包率增加了 0.34%. 其主要原因是: Web 流量必须通过 FW 和 WAF 进行检查和过滤, 才能转发到服务域中的网站服务器. 在这个过程中, 流量需要匹配 FW 中的数百个过滤规则和 WAF 中的数千个签名, 从而导致增加的延迟和减少的吞吐量. 在没有网络安全服务的情况下, Web 流量直接访问网站服务器, 以避免在系统开销方面进行检查. 因此, 与没有网络安全服务的情况相比, CNS 的延迟变长, 吞吐量受到延迟的影响, 但是增加网络安全服务后的整体系统性能在可接受的范围内.

以 Web 服务为例. 检测该系统的防攻击能力, 针对 Web 的网络层进行了 IP 攻击、DDOS 攻击以及使用了扫描器, 表 7 的实验结果表明该系统均能检测出攻击且成功进行防护. 针对 Web 的应用层进行了远程登录攻击、cookies 欺骗和 SQL 注入, 表 7 的实验结果表明, 该系统均能检测出攻击且成功进行防护, 验证了本文方法在安全防护上的效果.

表 7 Web 服务攻击防护验证

| 攻击软件 | 攻击对象 | 攻击说明 | 检测情况 | 防护情况 |
|---|---|---|---|---|
| NTHunterV2.0 | Web 网络层 | IP 攻击 | √ | √ |
| DDOSIM-layer | Web 网络层 | DDOS 攻击 | √ | √ |
| X-way2.5 | Web 网络层 | 扫描器 | √ | √ |
| Opentelnet | Web 应用层 | 远程登录入侵 | √ | √ |
| IEcookiesView | Web 应用层 | Cookies 欺骗 | √ | √ |
| Havij | Web 应用层 | SQL 注入 | √ | √ |

## 4 结论

在云计算服务中, 如果不采取保护措施来保护网络安全, 可能导致无法估量的损失, 然而传统的安全模式无法提供个性化的安全服务, 不能满足医疗健康云用户安全需求的多样性, 本文提出面向健康云的定制化网络安全服务可以自动根据云用户安全需求提供相应的安全服务, 同时也提供了攻击日志和统一管理功能, 保证安全的同时也能减少人力财力的开销. 延迟增加、吞吐量降低、丢包率增加等网络安全服务带来的负面因素, 因此未来可以进一步探索的工作是如何把网络安全服务在性能上的开销控制接受范围内即可.

## 参考文献


1 Takabi H, Joshi JBD, Ahn GJ. Security and privacy challenges in cloud computing environments. IEEE Security & Privacy, 2010, 8(6): 24–31.
2 沈志荣, 薛巍, 舒继武. 可搜索加密机制研究与进展. 软件学报, 2014, 25(4): 880–895.
3 Cao N, Wang C, Li M, *et al*. Privacy-preserving multi-keyword ranked search over encrypted cloud data. Proceedings of 2011 IEEE INFOCOM. Shanghai, China. 2011. 829–837.
4 何进, 范明钰, 王光卫. 自动探测和保护确保内核完整性. 电子科技大学学报, 2014, 43(4): 585–590.
5 李攀攀. 云服务 SLA 合规性验证及性能优化研究[博士学位论文]. 哈尔滨: 哈尔滨工业大学, 2016.
6 刘世辉. 基于 SDN 和 NFV 的链路洪泛攻击检测与防御[硕士学位论文]. 武汉: 武汉大学, 2017.
7 Zissis D, Lekkas D. Addressing cloud computing security issues. Future Generation Computer Systems, 2012, 28(3): 583–592. [doi: 10.1016/j.future.2010.12.006]
8 Subashini S, Kavitha V. A survey on security issues in service delivery models of cloud computing. Journal of Network and Computer Applications, 2011, 34(1): 1–11. [doi: 10.1016/j.jnca.2010.07.006]
9 He J, Dong MX, Ota K, *et al*. NetSecCC: A scalable and fault-tolerant architecture for cloud computing security. Peer-to-Peer Networking and Applications, 2016, 9(1): 67–81. [doi: 10.1007/s12083-014-0314-y]
10 Lin CH, Tien CW, Pao HK. Efficient and effective NIDS for cloud virtualization environment. Proceedings of the 4th IEEE International Conference on Cloud Computing Technology and Science. Taipei, China. 2012. 249–254.
11 Nguyen A, Raj H, Rayanchu S, *et al*. Delusional boot: Securing hypervisors without massive re-engineering. Proceedings of the 7th ACM European Conference on Computer Systems. Bern, Switzerland. 2012. 141–154.
12 Fayazbakhsh SK, Sekar V, Yu ML, *et al*. FlowTags: Enforcing network-wide policies in the presence of dynamic middlebox actions. Proceedings of the 2nd ACM SIGCOMM Workshop on Hot Topics in Software Defined Networking. Hong Kong, China. 2013. 19–24.
13 Fayazbakhsh SK, Chiang L, Sekar V, *et al*. Enforcing network-wide policies in the presence of dynamic middlebox actions using flowtags. Proceedings of the 11th USENIX Conference on Networked Systems Design and Implementation. Seattle, WA, USA. 2014. 533–546.
14 Sekar V, Ratnasamy S, Reiter MK, *et al*. The middlebox manifesto: Enabling innovation in middlebox deployment. Proceedings of the 10th ACM Workshop on Hot Topics in Networks. Cambridge, Britain. 2011. 21.
15 He J, Ota K, Dong MX, *et al*. Customized network security for cloud service. IEEE Transactions on Services Computing, 1939, PP(99): 1–1. [doi: 10.1109/TSC.2017.2725828]