计算机系统应用 ISSN 1003-3254, CODEN CSAOBN
Computer Systems & Applications,2019,28(12):212−218 [doi: 10.15888/j.cnki.csa.007201]

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

交换机 ACL 在 WWW 服务器安全防护中的应用①

单庆元, 阎丕涛, 南　峰

(大连工业大学 网络信息中心, 大连 116034)
通讯作者: 单庆元, E-mail: shanqy@dlpu.edu.cn

摘　要: 为了解决服务器系统及软件自身安全设置在服务器被入侵后可被重置, 以及用于面防护的安全设备 (硬件防火墙等) 安全防护粒度大的问题, 通过分析 WWW 服务器常用的网络应用如: WWW、DNS、FTP 等, 总结出各个网络应用数据流的特征, 使用动态端口固定化原则和动态管理 IP 固定化原则, 并据此配置服务器接入交换机 ACL (访问控制列表), 并将针对于每个服务器的 ACL 应用于服务器连接的交换机端口, 对服务器进行点防护. 在服务器防火墙规则禁用的情况下, 服务器接入交换机 ACL 能够对服务器的行为进行限制, 进而保护了服务器和内网网络设备. 使用基于 INTEL DPDK (数据平面开发工具) 的 Pktgen 发包工具进行测试, 服务器接入交换机 ACL 能很好的过滤掉服务器发出的高并发、大流量的异常数据包, 进而保护了网络和设备.

关键词: 访问控制列表; 网络服务; TCP 端口; 服务器防护

引用格式: 单庆元,阎丕涛,南峰.交换机 ACL 在 WWW 服务器安全防护中的应用.计算机系统应用,2019,28(12):212–218. http://www.c-s-a.org.cn/1003-3254/7201.html

Application of Switch ACL in WWW Server Security Protection

SHAN Qing-Yuan, YAN Pi-Tao, NAN Feng

(Network Information Center, Dalian Polytechnic University, Dalian 116034, China)

Abstract: This study is designated to solve the problem of that server system and software's security configurations can be reset after the server is invaded, and the network security equipment (hardware firewall, etc.) has large granularity. We analyze common network applications of WWW server, such as WWW, DNS, and FTP, summarize of the characteristics of each network application protocol, and according to the principle of dynamic port fixation and dynamic managerment IP fixation, configure the server access switch ACL, then apply each server's ACL to the server-connected switch port, protect the server specially. When the server firewall rules are disabled, the server access switch ACL can limit the behavior of the server, thus protecting the servers and the intranet network devices. Using the Pktgen tool based on INTEL DPDK (Data Plane Development Tool) to test, ACL in the server access switch can filter the high abnormal traffic from the server and protect the network and equipment.

Key words: ACL; network service; TCP port; server protection

统计显示, 黑客入侵主机后, 在一段时间内能够在主机上潜伏而不被发现, 在这样的情况下, 限制一台服务器在被入侵之后的行为就变得很重要. 而服务器的安全措施通常有两类: ① 服务器系统及软件本身的安全设置[1]. ② 位于服务器之外的安全设备 (例如: 防火墙、应用安全网关等) 的防护[2]. 由于服务器本身的安

① 收稿时间: 2019-05-17; 修改时间: 2019-06-21; 采用时间: 2019-06-25; csa 在线出版时间: 2019-12-10

全策略在系统被入侵后有被清除的风险, 而安全设备由于价格的原因, 通常用于对一定网络区域 (例如: 全部服务器或内网) 的防护, 所以被入侵服务器会对安全设备保护之下的内网设备造成影响. 被入侵设备通常被当成网络入侵中继点, 去扫描其它的设备, 而扫描而形成的巨大的并发连接及网络流量通常会占用很大的出口带宽、消耗过多出口安全设备的处理性能, 形成拒绝服务攻击, 使网络处于瘫痪状态. 针对上述两种服务器防护措施的不足, 通过对服务器应用数据包的分析, 可利用交换机 ACL 对每台服务器的网络访问进行限制. 由于接入交换机 ACL 具有高效 (基于硬件的过滤机制, 可达线性的流量处理)、专用 (ACL 可针对每个服务器设置和应用, 防护粒度小)、廉价 (接入交换机价格便宜) 的特点, 而且服务器无法更改交换机配置. 因此, 通过增加接入交换机 ACL 对服务器进行防护, 可以有效地保护服务器和降低被入侵服务器对网络造成的影响.

1 WWW 服务器常用服务分析

由于交换机 ACL 非防火墙应用规则, 不监控网络连接所处的状态, ACL 只是根据每条 ACL 的内容检查网络数据包, 根据规则的设置执行指定的动作. 配置及应用交换机 ACL 的前提是对网络应用连接的透彻分析, 总结出每个应用的访问连接的特点, 并据此编写 ACL 的规则. 本次试验的 WWW 服务器特点如下: WWW 服务器的 IP 地址为 WWW_SERVER_IP, 操作系统是 WINDOWS; 使用微软的 IIS 提供 WWW 服务; 使用 Filezilla 提供 FTP 服务; 为保证服务器日志时间的准确性, 使用了 NTP 客户端更新系统的时钟; 安装了杀毒软件; 对管理主机开放了 WINDOWS 远程桌面服务.

1.1 WWW 服务

在服务器端由软件服务程序 (例如: 微软的 IIS 服务器) 监听 WWW 服务端口 (通常为 TCP 80 端口, 但不限于该端口), 被动的接收来自 WEB 客户端 (通常为互联网浏览器) 的连接请求, 网络连接分析如表 1 所示.

表 1 WWW 服务的连接分析

作用	连接类型	本地 IP	本地端口	远程 IP	远程端口
WWW 服务发布	被动	服务器 IP	80	不固定	不固定

1.2 域名解析 (DNS) 服务

域名解析服务[3]是一种将便于用户记忆的网络域名转换成特定 IP 地址的服务 (例如: 将域名 WWW.DLPU.EDU.CN 转换成 IP 地址 210.30.48.9). 域名解析客户端软件通常向服务器的 UDP 53 端口发送解析请求, DNS 服务器将最终的解析结果通过该端口返回客户机. 网络连接分析如表 2 所示.

表 2 域名解析的连接分析

作用	连接类型	本地 IP	本地端口	远程 IP	远程端口
发送域名解析请求	主动	服务器 IP	不固定	DNS 服务器 IP	53

1.3 文件传输服务 (随机端口固定化原则)

FTP 服务[4]是常用的服务器和客户端之间传送文件的服务, FTP 服务器的操作命令的传输 (命令通道) 和数据的传输 (数据通道) 是通过不同的 TCP 端口来进行的. 命令通道通常在 TCP 21 端口接收客户的命令和返回结果. 数据通道有点特殊, 分为主动模式和被动模式. 主动模式是指服务器主动通过 TCP 20 端口连接客户机在命令通道中指定端口进行数据传输; 被动模式是指客户机主动连接服务器指定的端口进行数据传输, 通常这些端口是有服务器随机指定的, 这使得 ACL 无法配置. 为了解决此问题, FileZilla FTP 服务器提供了配置接口, 管理员可以指定被动模式下使用的端口范围[5]. 这可称之为: 随机端口固定化原则. 为了便于 ACL 配置, 设置服务器将 FTP 被动模式使用的随机端口固定下来, 使用 TCP 20001-20010, 网络连接分析如表 3 所示.

表 3 文件传输服务连接分析

作用	连接类型	本地 IP	本地端口	远程 IP	远程端口
命令通道	被动	服务器 IP	21	管理主机	不固定
主动模式数据通道	主动	服务器 IP	20	管理主机	不固定
被动模式数据通道	被动	服务器 IP	20001-20010	管理主机	不固定

1.4 服务器远程维护 (动态管理 IP 固定化原则)

服务器的远程维护对于服务器管理员来说是必须的, 通常的远程管理软件有微软自带的远程终端 (WINDOWS 系统)、赛门铁克公司的 PC ANYWHERE

(WINDOWS 系统), 这些软件默认所使用的端口都是固定的, 网络连接分析如表 4 所示.

表 4 远程维护连接分析

作用	连接类型	本地 IP	本地端口	远程 IP	远程端口
Windows 远程桌面	被动	服务器 IP	3389	管理主机	不固定
PC ANYWHERE	被动	服务器 IP	5631, 5632	管理主机	不固定

管理 IP 地址的不固定给 ACL 的配置带来了困难, 如果在 ACL 中不限制远程管理客户机的 IP 地址, 管理员维护方便, 带来的问题是网络上任何终端都可以尝试登录, 这不安全. 如果限制了管理客户机的 IP 地址, 管理员维护便利性就会下降, 而且如果管理员换管理主机, 就需要修改 ACL, 这不方便. 在这里, 可以增加一台 VPN 设备来解决这个问题. 管理员首先通过账号登录 VPN 设备, VPN 设备给管理员分配一个固定的 IP 地址, 在 ACL 里限制只有该固定 IP 地址可以远程管理服务器, 这样管理员在任何地方都可以通过先登录 VPN, 然后管理服务器了. 这可称为: 动态管理 IP 固定化原则. 并且只有知道 VPN 用户名、密码、服务器远程 IP 地址以及服务器的用户名、密码才能登录服务器, 安全性和便利性都可兼顾.

1.5 防病毒类软件升级服务

在服务器中也经常遇到特征库的升级问题, 例如: 反病毒库、应用特征库、垃圾邮件库等等, 如果这些特征库不升级, 那么应用服务运行的效果会差很多. 为了保障应用运行的效果, 需要配置 ACL, 使得特征库能正常升级. 网络连接分析如表 5 所示.

表 5 反病毒软件升级服务

作用	连接类型	本地 IP	本地端口	远程 IP	远程端口
特征库升级	主动	服务器 IP	不固定	升级服务器	80 或 443

这里仅列出了部分常见应用的网络连接, 对于其它的服务, 可以自己完成协议分析.

2 WWW 服务器 ACL 配置及分析

经过上面对应用协议的分析, 掌握了应用正常运行所必须开放的端口, 可以据此配置交换机的 ACL, 下面是 WWW 服务器的交换机 ACL 配置实例.

2.1 WWW 服务器 ACL 配置

本次试验所使用的交换机型号为锐捷网络的 S2928G-24P, 软件版本为: RGOS 10.4(2b12)p6 Release (196987), 首先需要根据第 2 小节的网络连接分析, 配置一个名称为 for_http 的 ACL, 该 ACL 的内容如表 6 所示.

表 6 ACL 的内容

序号	ACL 列表项
1	ip access-list extended for_http
2	permit tcp WWW_SERVER_IP eq 80 any
3	permit tcp WWW_SERVER_IP eq 21 host 管理主机 IP
4	permit tcp WWW_SERVER_IP range 20001 20010 host 管理主机 IP
5	permit tcp WWW_SERVER_IP eq 20 host 管理主机 IP
6	permit tcp WWW_SERVER_IP eq 3389 host 管理主机 IP
7	permit tcp WWW_SERVER_IP host 病毒库升级服务器 IP eq 80
8	permit udp WWW_SERVER_IP host DNS_SERVER_IP eq 53
9	permit udp WWW_SERVER_IP host NTP_SERVER_IP eq 123
10	deny ip any any

表 6 中的 ACL 表项的按序号解释如下: ① 定义一个名为 for_http 的扩展的访问控制列表; ② 允许源地址为 WWW_SERVER_IP, 源端口为 TCP 80, 目标地址为任意的数据包转发. 作用: 开放服务器的 WWW 服务; ③ 允许源地址为 WWW_SERVER_IP, 源端口为 TCP 21, 目标地址为管理主机 IP 的数据包转发. 作用: 开放服务器 FTP 服务的命令通道; ④ 允许源地址为 WWW_SERVER_IP, 源端口范围为 TCP 20001-20010, 目标地址为管理主机 IP 的数据包转发. 作用: 开放服务器 FTP 服务的被动模式数据通道; ⑤ 允许源地址为 WWW_SERVER_IP, 源端口为 TCP 20, 目标地址为管理主机 IP 的数据包转发. 作用: 开放服务器 FTP 服务的主动模式数据通道; ⑥ 允许源地址为 WWW_SERVER_IP, 源端口为 TCP 3389, 目标地址为管理主机 IP 的数据包转发. 作用: 允许管理主机访问服务器的远程桌面服务; ⑦ 允许源地址为 WWW_SERVER_IP, 目标地址为病毒库升级服务器 IP, 目标端口为 TCP 80 的数据包转发. 作用: 允许服务器的病毒软件进行更新病毒库; ⑧ 允许源地址为 WWW_SERVER_IP, 目标地址为 DNS_SERVER_IP, 目标端口为 UDP 53 的数据包转发. 作用: 允许服务器进行域名解析; ⑨ 允许源地址为 WWW_SERVER_IP, 目标地址为 NTP_SERVER_IP, 目标端口为 UDP 123 的数据包转发. 作用: 允许服务器进行时间更新; ⑩ 拒绝任何 IP 数据包转发. 作用: 除了上述指定的数据包可以转发外, 其它的 IP 数据包全部

丢包. 注: 在配置时, 表 6 中的“管理主机 IP”、“病毒库升级服务器 IP”、“DNS_SERVER_IP”、“NTP_SERVER_IP”需要用真实的 IP 来替换.

最后将该访问控制列表应用于 WWW 服务器连接的交换机的接口的 IN 方向, 对 WWW 服务器发送的, 进入交换机的数据包进行过滤.

3 WWW 服务器 ACL 运行分析

3.1 交换机接口入向的 ACL 处理逻辑流程[6]

交换机接口入向的 ACL 处理逻辑流程如图 1 所示.

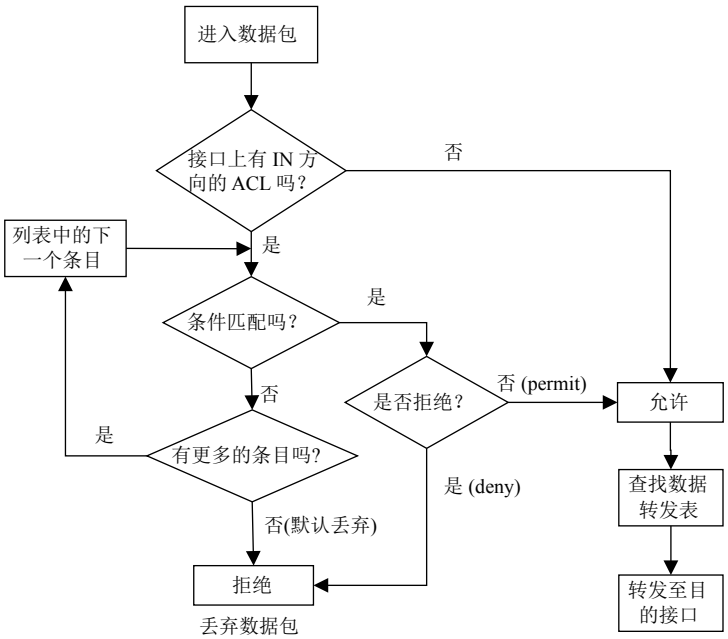

图 1 IN 方向的 ACL 流程图

从图 1 可以看出, 当交换机的某个接口收到一个数据包之后, 交换机首先检查该接口的 IN 方向是否应用了 ACL, 如果没有应用 ACL, 那么交换机查找转发表, 将数据包转发至相应接口. 如果该接口 IN 方向应用了 ACL, 那么进入 ACL 表项的比对过程. ACL 实行首次匹配策略, 从第一条规则开始, 进行比对, 当数据包匹配该条规则后, 如果规则的动作是 permit, 数据包会被转发, 如果规则的动作是 deny, 数据包会被丢弃, 不再检查后续的规则. 如果不匹配当前的规则, 那么继续比对下一条规则, 直至最后的默认规则. 每个 IP 数据包肯定会匹配一条规则, 因为每个 ACL 最后会有一条默认规则, 该规则匹配任何的 IP 数据包, 匹配后的动作是丢弃数据包.

3.2 交换机 ACL 对服务器及内网设备的保护分析

很多的情况下, 由于管理不善, 服务器管理员随意地使用服务器去浏览互联网的资源、安装与服务无关的应用, 导致服务器运行缓慢, 甚至崩溃. 使用表 6 的交换机 ACL 可以禁止服务器访问互联网的应用和资源. 原理如下: 当用户使用服务器访问某个网站时 (这里以 WWW.BAIDU.COM 为例), 由于 ACL 第 8 条规则的作用, 服务器可以成功的把域名转换成 IP 地址 (域名 WWW.BAIDU.COM 对应的 IP 地址为: 119.75.216.20), 然后服务器上应用 (例如: 浏览器) 发送一个 TCP 连接状态请求的数据包, 数据封包的源 IP 为 WWW_SERVER_IP, 目标地址为 119.75.216.20, 源端口随机生成, 现假设为 TCP 1850, 目标端口为 TCP 80, 同时 TCP 连接标志 TCP Flags 中的 SYN 位置为 1, Sequence Number 为 x; 然后, 服务器进入 SYN_SEND 状态, 等待 119.75.216.20 的确认. 当交换机接收到该数据包时, 进入 IN 方向的 ACL 检查过程, 由于 ACL 的 2-9 项都不能匹配该数据包, 则匹配所有 IP 数据包的第 10 项匹配成功, 该数据包被丢弃. 所以 IP 为 119.75.216.20 的服务器不会收到 WWW 服务器的连接请求, 而 WWW 服务器更不会收到连接响应, 最终该连接因超时而失败. 由于服务器无法访问互联网资源, 无法使用与服务无关的联网应用, 因此服务器的安全性会有很大提升.

成功入侵服务器后潜伏下来黑客, 会利用被入侵的服务器作为中介, 去扫描内网的设备, 以获取内网设备信息, 或者操控服务器进行 DDOS 攻击. 在服务器上

使用网络扫描软件对内网进行扫的数据包和服务器对外的 DDOS 攻击的数据包也会因为只能匹配 ACL 的第 10 项而被丢弃, 所以很好地保护了内网的设备安全.

另外, 访问控制列表一般由交换机芯片中的 TCAM[7−9]来实现, 可实现过滤条件下线速转发, 交换机 ACL 能把从服务器发出的大流量、高并发的恶意扫描数据包过虑掉, 且不影响正常的数据转发.

4 基于 INTEL DPDK 和 PKTGEN 工具的测试

为了测试交换机 ACL 在大流量、高并发的数据流量下的处理情况, 使用基于 INTEL DPDK[10,11]的 PKTGEN 的软件进行模拟的发包测试, DPDK 使用用户态的网卡驱动、轮询 (polling) 模式、内存大页等多种技术[12,13]极大提升了系统的包处理速率. 本次测试使用的软件为: dpdk-stable-18.02.tar.gz, pktgen-dpdk-pktgen-3.5.0.tar.gz 下载地址是: https://git.dpdk.org/, 本次测试使用的设备配置如表 7 所示.

表 7 测试设备配置信息

设备名称	硬件配置	软件配置
台式机	CPU: Intel Core i5-2300 CPU @ 2.80 GHz、内存: 4096 M DDR3 1333 MHz、网卡: Intel 82580 I340-T4 E1G44HT PCI-E 四端口网卡	操作系统: Centos7.0、dpdk-stable-18.02、pktgen-dpdk-pktgen-3.5.0
交换机	锐捷 S2928G-24P	RGOS 10.4(2b12)p6 Release(196987)
笔记本电脑	CPU: Intel i7-8550U CPU @ 1.80 GHz、内存: 8192 M 2400 MHz、网卡: Realtek 千兆网卡	操作系统: 64 位 win10 家庭中文版、wireshark 2.6.3

测试拓扑如图 2 所示.

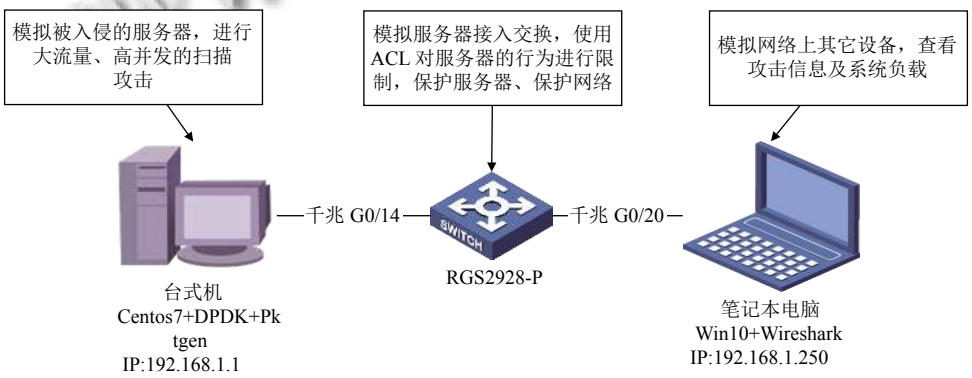

图 2 测试拓扑

软件的安装请参考 https://www.dpdk.org/, DPDK 和 pktgen 安装完成后, 通过以下命令配置运行环境并启动发包测试:

echo 1024 > /sys/kernel/mm/hugepages/hugepages-2048kB/nr_hugepages 注: 设置内存大页

mkdir /mnt/huge/

mount -t hugetlbfs nodev /mnt/huge/

modprobe uio 注: 加载用户空间 IO 模块

insmod /root/dpdk/lib/modules/3.10.0-862.el7.x86_64/extra/dpdk/igb_uio.ko 注: 加载 UIO 网卡驱动

/root/dpdk/share/dpdk/usertools/dpdk-devbind.py –status 注: 查看系统中网卡状态

/root/dpdk/share/dpdk/usertools/dpdk-devbind.py -b igb_uio 0000:02:00.0

cd /root/pktgen-dpdk-pktgen-3.5.0

注: 进入 pktgen 安装目录

/root/pktgen-dpdk-pktgen-3.5.0/app/x86_64-native-linuxapp-gcc/pktgen-c f --master-lcore 0 -n 4 -m 1024 --proc-type auto --file-prefix pg -- -m"1.0"

注: 运行软件

set 0 type ipv4

注: 设置 0 号网卡发送 IPV4 数据包

set 0 proto udp

注: 使用 UDP 协议 默认源端口: 1234 目的端口: 5678

set 0 count 0 注: 不间断发包

set 0 size 64 注: 包大小为 64 字节

set 0 pattern none 注: 不指定包填充模式

set 0 dst mac d8:c4:97:93:5a:6a

注: 设置发包的目的为笔记本电脑 mac 地址

set 0 src ip 192.168.1.1/24

注: 设置发包的源 IP 地址

set 0 dst ip 192.168.1.250

注: 发包的目的为笔记本电脑 IP 地址

set 0 rate 100 注: 发包速率, 满负荷发包

start 0 注: 启动 0 号网卡发包

发包开始之后, 通过交换机的命令 show cpu; show memory; show interface counters rate 分别查看交换机 CPU 的使用率、内存的使用率、G0/14 接口和 G0/20 接口的收发包的统计数据 (5 分钟均值). 从发包开始, 以上命令总共运行了 313 次, 第 254 次命令运行后 (图中箭头所指处), 在 G0/14 接口的 IN 方向应用如下的访问控制列表:

ip access-list extended for_http

permit tcp host 192.168.1.1 eq 80 any

permit tcp host 192.168.1.1 eq 21 host 192.168.1.100

permit tcp host 192.168.1.1 range 20001 20010 host 192.168.1.100

permit tcp host 192.168.1.1 eq 20 host 192.168.1.100

permit tcp host 192.168.1.1 eq 3389 host 192.168.1.100

permit udp host 192.168.1.1 host 192.168.1.7 eq 53

permit udp host 192.168.1.1 host 192.168.1.24 eq 123

deny ip any any

交换机的上述 3 个 show 命令的输出数据如图 3.

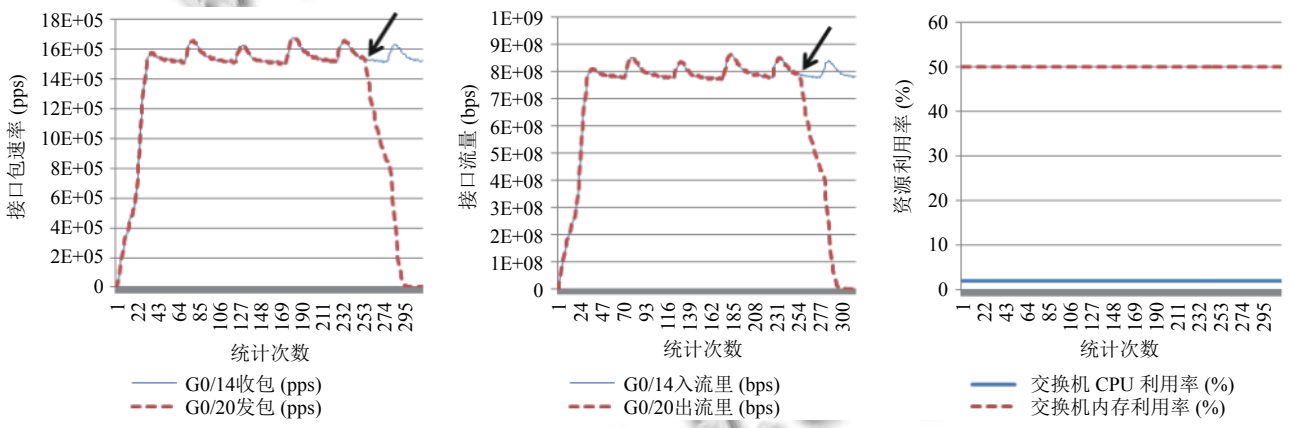

图 3 交换机接口流量及资源利用率

图 3 的左边 (中间) 分别是 G0/14 接口收包速率 (收包流量) 和 G0/20 接口的发包速率 (流量) 的统计, 单位为 PPS (bps), 在 PC 机启动发包测试后, G0/14 接口收包速率 (收包流量) 和 G/20 接口发包速率 (发包流量) 从 0 开始, 经过快速上升后, 在 150 万 PPS (783M bps) 和 168 万 PPS (860M bps) 之间波动, 且在箭头所指点之前, G0/14 接口的收包速率 (收包流量) 和 G0/20 接口的发包速率 (发包流量) 是同步的, PC 发送给笔记本的数据都被交换机正常转发了. 在箭头所指处, 由于在 G0/14 接口的 IN 方向应用了访问控制列表, G0/20 接口的输出迅速降为零, 尽管此时 PC 机依旧不停地发包. 由于交换机的查看命令输出的是 5 分钟均值, 所以在图中可以看到一个下降过程, 实际上当应用访问控制列表后, 笔记本就不再收到 PC 机发送的数据包了. 图 3 的右边是交换机资源的利用率, 在访问控制列表应用前后, 交换机 CPU 和内存的使用无任何变化.

5 结论

服务器接入交换机在网络防护中有着重要的作用, 在接入服务器交换机上 ACL 可以单独针对特定服务器配置. 通过对应用及协议进行透彻的分析, 总结出规律, 使用动态端口固定化原则和动态管理主机 IP 固定化原则, 可以将一些服务中不固定的参数固定下来. 另外在管理主机 IP 地址固定化时需要 VPN 设备, 这需

要一定的费用, 因为在特定的科技条件下, 安全性、便利性和经济性往往不可兼得, 只能根据需求在每个方面进行取舍. 另外本次实验中, 只是对服务器发出的数据包进行控制, 网络上其它主机发送给服务器的数据包还是能够正常转发至服务器, 如果恶意主机给服务器发送大量的或者是异常的数据包, 并且服务器主机防火墙设置不合理, 可能会造成服务器异常. 对于这种情况, 可以在交换机上同时对服务器 IN 和 OUT 方向的数据包进行过滤, 这样只有客户机正常的服务请求数据包才能发送至服务器, 不足之处就是消耗了较多的交换机 ACL 资源.

参考文献

1 陈彬. 互联网服务器攻防秘笈. 北京: 化学工业出版社, 2011.

2 张丹东. 多手段防护 WEB 安全. 中国教育网络, 2017, (6): 25–26.

3 Albitz P, Liu C. DNS and BIND. 5th ed. Sebastopol, CA: O'Reilly, 2001.

4 谢希仁. 计算机网络. 5 版. 北京: 电子工业出版社, 2008.

5 Filezilla Project. Network configuration. https://wiki.filezilla-project.org/. [2017-05-01].

6 Ruijie Corporation. ACL 与包过滤. http://www.ruijie.com.cn/. [2017-07-21].

7 刘中金, 李勇, 苏厉, 等. TCAM 存储高效的 OpenFlow 多级流表映射机制. 清华大学学报 (自然科学版), 2014, 54(4): 437–442.

8 费宁, 陈春玲, 毛燕琴. ASIC 芯片 OpenFlow 交换机设计与实现. 北京邮电大学学报, 2016, 39(6): 93–98.

9 Huawei Corporation. Huawei CloudEngine 系列交换机_ACL 技术专题. http://support.huawei.com/onlinetoolweb/dataCommunication/zh/DC/technology.html. [2018-11-07].

10 朱可清, 梁存铭, 胡雪焜, 等. 深入浅出 DPDK. 北京: 机械工业出版社, 2016.

11 Dpdk project charter. https://www.dpdk.org/. [2018-05-01].

12 任昊哲, 年梅. 基于 DPDK 的高速数据包捕获方法. 计算机系统应用, 2018, 27(6): 240–243. [doi: 10.15888/j.cnki.csa.006388]

13 李霞, 李虎, 甘琤, 等. 服务器中高性能网络数据包处理方法的对比研究. 计算机应用与软件, 2017, 34(11): 177–183. [doi: 10.3969/j.issn.1000-386x.2017.11.033]