计算机系统应用 ISSN 1003-3254, CODEN CSAOBN
Computer Systems & Applications,2020,29(4):144−149 [doi: 10.15888/j.cnki.csa.007360]

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

高性能公有云 WAF 安全方案①

何　丹[1], 张　悦[2]

[1](中移 (苏州) 软件技术有限公司 云计算产品部, 苏州 215000)
[2](中移 (苏州) 软件技术有限公司 大数据产品部, 苏州 215000)
通讯作者: 何　丹, E-mail: dandanho@126.com

摘　要: 高性能云化 WAF 方案在 WAF 流量防护监测上设计了各个处理流程之间的协同调整处理能力以及同步机制, 实现了处理步骤之间的能力相互感知, 动态变化能力高效协同, 解决了传统方案防护效率低的问题. 另一方面高性能云化 WAF 方案在防护引流拓扑上设计了 SDN 牵引流量和策略下发分离, 实现了 WAF 的并发防护调用, 解决了传统方案防护吞吐量低的问题. 实验表明高性能云化 WAF 方案对比传统云 WAF 防护方案有较高的防护效率, 较高的防护吞吐量.

关键词: WAF; 流量监控统计; 并发拓扑; 引流

引用格式: 何丹,张悦.高性能公有云 WAF 安全方案.计算机系统应用,2020,29(4):144–149. http://www.c-s-a.org.cn/1003-3254/7360.html

High Performance WAF Security Scheme in Cloud Computing

HE Dan[1], ZHANG Yue[2]

[1](Cloud Computing Sector, ChinaMobile (Suzhou) Software Technology Co. Ltd., Suzhou 215000, China)
[2](Big Data Sector, ChinaMobile (Suzhou) Software Technology Co. Ltd., Suzhou 215000, China)

Abstract: By introducing an efficient statistical scheme for WAF traffic analysis processing which provides a mechanism for each processing Flow to dynamically adjust the processing capability, realizes dynamic adjustment processing capability, and realizes coordination adjustment processing capability and the synchronization mechanism between the various processing. On the other hand, in the traditional topology, drainage is started by the virtual network of the host machine or started by a stream serial thread with SDN. By introducing the high concurrent traction scheme in this study, the SDN traction Flow, strategy downward separation, and the concurrent protection of WAF are realized. Experimental results show that the scheme improves the accuracy of WAF protection and improves the WAF throughput.

Key words: WAF; traffic statistics; concurrent topological; drainage

1　引言

WAF (Web Application Firewall) 是 Web 网络应用防护系统, 担当着是 Web 应用的防护, 由于现如今 Web 应用在当今互联网应用中的主流应用, 一般来说 WAF 的应用防护包括一般包括常见的 Web 防护, 比如异常的流量监测、DDoS 攻击、https 攻击、SQL 注入的攻击、命令注入攻击、cookie/seesion 劫持、应用平台攻击劫持等攻击[1]. 而这些业界对全面防护能力的要求都离不开专业的 WAF 设备防护以及流量防护方案.

而云计算业务的应用越来越普及, 行业内的企业和单位已经将自己的 Web 业务信息系统逐渐的迁移至云服务中. 集中化的云虚机部, 使得部署资源的集中化. 这些企事业单位享受着云化业务带来的好处的同时, 其集中化云 Web 服务的安全无疑是最大的挑战[2], 然而集中化的云端部署, 也为 WAF 防护应用的发挥提供了舞台.

① 基金项目: 中国移动公有云项目 (C201985-096)
Foundation item: China Mobile Public Cloud Project (C201985-096)
收稿时间: 2019-09-08; 修改时间: 2019-10-08; 采用时间: 2019-10-22; csa 在线出版时间: 2020-04-05

业界公有云提供云内 WAF 安全框架如图 1, 将云内 Web 流量先交由专业 WAF 设备来防护清洗.

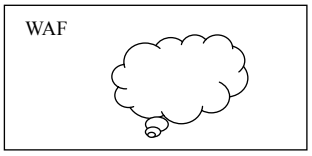

图 1 云内 WAF 防护

2 业界 WAF 方案分析

中国移动在全国布局公有云 WAF 应用中, 发现业界方案在流量防护效率、整体引流拓扑防护吞吐量表现不足.

2.1 流量监测现状

WAF 防护系统在做流量防护的时候, 需要时刻对流量进行检测分析. 而流量监控分析的功能是采集交换机不断的生成 Flow, 并将采集后的 Flow 流的拆包解析、归并. 流量监测分析技术实现的是对高速转发的网络层 IP 数据流流量信息进行采集, Flow 提供的是网络流量的会话级视图, 这种会话级视图, 可以定义为包含一个源 IP 地址和目的 IP 地址间传输的数据包流数据交换形式.

这种业界 Flow 流的串行分析流程, 存在以下问题:

首先, 接收 Flow 步骤和解析 Flow 步骤以及归并计算步骤其处理能力被设定预设固定值. 无法动态自适应调整处理能力.

其次, 对着图 2 的处理步骤, 整体流量监控机制缺乏收集能力与解析能力之间的协同同步机制, 以及缺乏接收能力和解析能力两者之间的协同同步机制. 每个处理步骤无法感知其上游处理业务压力及下游步骤处理能力.

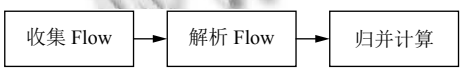

图 2 WAF 流量解析过程

上述缺陷, 或者由于上游步骤传过来的数据量较大, 而下游步骤的处理能力被固定的较小, 导致来不及接收, 来不及解析的丢包情况. 使得监控数据的丢失而降低防护的精度. 或者由于上游数据量较小, 而预置的下游步骤的处理能力被预设的很大, 导致等待接收, 等待解析的浪费计算资源情况. 而在突发大流量的 WAF 应用场景中, 这种流量监测机制通常会无法适应突发的统计数据量将流量丢弃, 影响中国移动云 WAF 的防御的效果.

2.2 引流拓扑现状

一般业务的防护系统 WAF, 如果云网络不是 SDN 网络, 需要通过流量代理的方式在云实现东西向流量的牵引调度: 将防护流量引流到 WAF 设备, 代理引流需要在部署机器中设置一个引流代理, 通过代理来将防护流量引入 WAF 设备. 通过在部署机器中集中的引流虚拟机接收防护策略, 并按照防护策略对流量进行牵引到 WAF 设备的一种拓扑, 拓扑中 WAF 的流量牵引为单线单 WAF 集群模式. 安全控制平台将相应的引流请求发送至这个引流代理, 引流代理根据虚拟机所在宿主机的位置以及虚拟机当前的网络情况, 下发相应的引流指令, 并且完成对应的网络配置, 实现流量牵引.

这种业界引流代理一方面在进行引流操作时, 需要获取对云计算系统较大的操作权限, 代理功能依赖于平台环境, 这样每种代理和云计算平台之间很难进行解耦[3], 而且代理的部署设置难以移植和进行部署复用. 另一方面这种单线的引流回大幅的增加图 3 左侧 vswitch 的负载. 拓扑中 WAF 的流量牵引为单线单 WAF 集群模式, 引流过程中需要占用大量的平台内部网络资源进行. 而且这种代理引流会使得操作依附于云计算平台, 使得操作复杂. 而业界 SDN 引流也为 4.1 介绍串行单线引流. 防护策略与流量牵引的串行结构使得策略与操作没有分离, 限制了 SDN 引流效率[4], 和 WAF 的防护吞吐率.

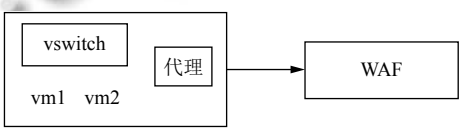

图 3 流量牵引

3 流量监测改造

本章设计流量监测改造方案解决 2.1 提出的流量监测低效问题, 方案包括设计 3.3 模型, 以及 3.4 改造算法. 方案提供了各个处理流程可动态化调整处理能力的机制, 实现自适应动态化调整处理能力, 解决了流量处理步骤能力固定的问题. 方案提供了同步算法, 使得各个处理流程之间的协同调整处理能力以及启动的同步机制, 实现了处理步骤之间的能力相互感知, 并动态变化能力以匹配高效协同, 解决了处理步骤能力配

合低效的问题.

3.1 流量统计监测

如 2.1 业内对流量解析的流程通过固定的格式包来解析所得到的对应 Flow 流, 并采用单步的收集过程, 而后进行归并计算. 整体流程的统计监测结果一般如图 4.

源地址	目的地址	源端口	网络名	协议类型	大小	默认
10.10.28.131	10.10.28.131	6443	other	17	684 430	1
10.10.28.133	10.10.28.131	6443	as6	17	14 500	1
10.10.28.134	10.10.28.131	6443	other	17	1570	1

图 4 流量统计监测

这是包含网络七元组的统计信息源地址、目的地址、源端口、协议类型、流量大小等. 这些信息都是可用提供 WAF 平台防 DDoS 或者其他功能的特征信息. DDoS 攻击会使得网络上出现可检测的统计性特征[5,6]: 比如一个网络真实节点的节点位置相对固定, 其地址的 TTL 值比较稳定, 由于 TTL 的值难以变动, 所以可以用来将其视为一个特征值来判定虚假的 IP 攻击行为; 比如 SYN Flood 类型的攻击中最明显的攻击特征就是由于虚假的 SYN 请求过多, 半连接剧烈增长, 而与之对应的 FIN 信号很少. 这种情况下可以具体设计将间隔时间内将 SYN 和 FIN 的比值作为阈值判断, 当 SYN 信号的数量超过 FIN 信号数量过多, 起比值超过阈值的时候可作为攻击特征; 另外访问攻击目标的源地址的新增 IP 数量剧烈上升特征, 也能做攻击判定.

3.2 流量解析模块

对流量解析具体的业界流程为例: 由图 2 显示在此过程中的收集 Flow 和归并计算按照流程分两步处理, 这样的设计在做流量监控的时候, 会导致性能上的缺陷. 首先 Flow 记录的发送能力和接受和收集 Flow 接受能力难以配和和协同. 在 Flow 记录高速大量的全部进行发送, 而此 Server 端没办法感知到 Flow 流的速度, 从而导致 Server 端无法全部解析 Flow 记录, 而无法计算解析的 Flow 包, 将会被当做流量冗余而被丢弃, 最终使得 Server 端的缺乏协同而丢失数据 Flow 而导致流量统计精度不足. 另一方面若 Flow 记录发生的量小, Server 端的处理能力被预置的很大, 会造成 Server 端的等待, 其预置的处理能力将会空置和浪费.

3.3 改造流量监测模型

本文提出高效流量统计方案所提出的解决方法和系统包括, 如图 5 所示.

1) 线程组模块 Server 端接收 Flow 的接收模块.

2) 线程组模块 Server 端解析 Flow 的解析模块.

3) 线程组模块 Server 端计算 Flow 归并计算模块.

以上 3 个处理步骤采用线程, 通过动态化的线程组, 进行实现动态能力自动调节.

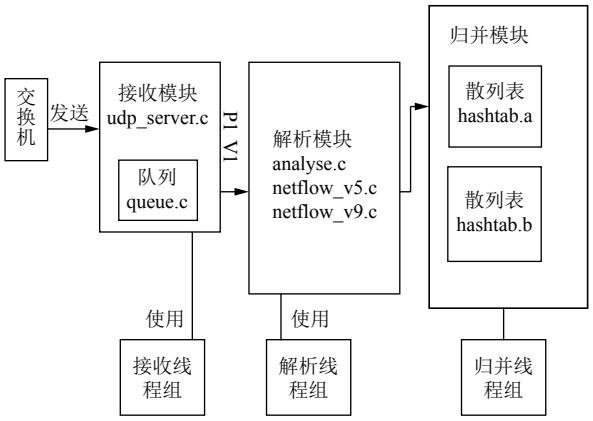

图 5 高性能流量监测流程

1) 如图所示定义 udpserver.c 的 Server 端的线程能力接收组, 以及 Server 端的解 analyse.c 的解析线程能力进程, 以及 Server 端的归并模块功能线程组.

2) 本功能模块组感知到不能够满足当前处理能力需求的时候, 比如当前解析线程数量为 n–1 模块解析速度较慢, 则本模块动态化处理能力增加处理能力资源, Server 端启动新线程 n 来提升解析速度, 此时的处理能力为使得模块处理速度达到 n.

3) 相反的当本模块能力感知能力为过剩的时候. 则同步算法要销毁最新启动的线程, 从而线程能力组的能力下降到 n–1, 释放单位的线程资源.

3.4 自适应统计同步算法详解

1) 在处理能力的适配上, 是根据处理能力需要自动调整的, 而处理能力大小的由信号量变量的值来决定. 接收线程通过 UDPserver 中的 recvfrom() 函数不断的循环监听抓取交换机发的 Flow 流. (Flow 流是 UDP 包), 并将 Flow 流写入长度为 n 的队列[7], 对于此队列长度 n, 如图 6 所示.

图 6 中接收步骤为生产者, 不断的往自己的队列塞从交换机那抓取的 Flow 记录, 解析模块从队列里面抽取, 成为消费者. 他们共享上述队列的资源池.

2) 设计算法的决策阈值, 本方案中设计高阈值为队列资源池的长度 n, 低阈值为空的队列资源池的长

度 0, 上图当生产者和消费者的之间的信号量作为两进程之间的线程组通信信号. 当步骤之间的信号量达到对应的阈值 n, 或者步骤之间的信号量达到对应的阈值 0, 则按照步骤 3) 的算法进行决策执行.

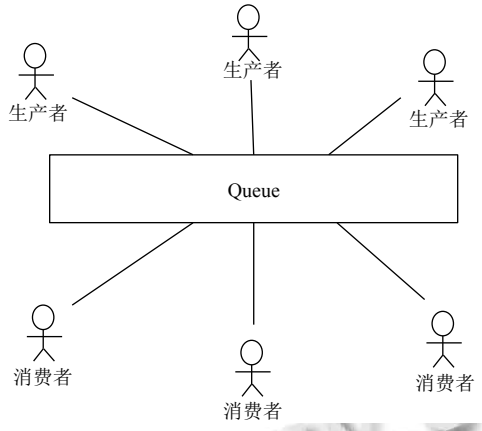

图 6 处理模块之间交互

3) 如果接收步骤过快, 步骤信号量达到满载的 n, 此时此发明启动设定增加消费者: 当此接收线程为 j, 解析线程为 i, 当 j 写入的数据数量 mi, mi 在 0~n 之间, mi 在每接收一个单位其值加 1, 在解析数据从队列取走数据解析时其值减 1, 当 mi 到达队列长度 n(写满) 则对解析步骤进行加速 (加大消费者能力速度) 此时解析步骤启动一个新线程 i+1. 此时阈值判断量为新的变量 n=mi+1.

4) 如果解析步骤过快, 步骤信号量达到空载的 0 此发明启动设定减少消费者: 当此发送线程为 j, 解析线程为 i, 当 j 写入的数据数量 mi, mi 在 0~n 之间, 到达队列长度 0(取空) 则对解析步骤进行减速 (降低消费者能力速度) 此时解析步骤销毁最新启动的当前线程 i. 此时阈值判断量为新的变量 n=mi–1.

5) 此算法的控制逻辑为图 5 中 P1V1 标记处通过信号量向后控制. 向后控制逻辑顺序类似栈结构: 写入相对过快则启动解析新线程顺序为解析 (1 号, 2 号, 3 号,…,i 号,i+1); 写入相对过慢则销毁的是当前解析线程号销毁顺序 (i 号, i–1 号,…,2 号,1 号).

4 引流拓扑改造

本章解决 2.2 业界的 WAF 的引流拓扑吞吐量低的问题: 业界 WAF 引流的 SDN 的引流方案为控制策略和流量承载都通过 SDN 网关来处理, SDN 网关可以通过代码接口用 NETCONF 协议进行控制配置, 比如下发路由实现流量牵引等, 7750 为诺基亚的 SDN 网关设备, 通过 7750 进行集中下发策略和承载引流, 使得控制过程和业务承载难以真正相互分离. 单一的防护资源池无法并发的进行流量的牵引. 导致防护吞吐量较低. 无法充分利用 WAF 的防护能力. 本章提出 WAF 引流拓扑改造, 实现 SDN 牵引流量承载和控制策略下发分离, 实现 WAF 的并发调用防护, 另一方面通过绕过 7750 的 SDN 对引流进行并发操作, 提高中国移动 WAF 设备使用效率, 提高 WAF 系统防护的吞吐能力.

4.1 WAF 的 SDN 引流拓扑

通过 SDN 集中的控制器, 来掌握整体的网络结构图[8–12]. 如果需要云平台里面的目标 Web 服务器进行防护, 需要进行检测和防护的流量, 方案的 SDN 完成流量的牵引的结构大概如图 7 所示: 以某厂商的云平台 SDN 引流方案为例子.

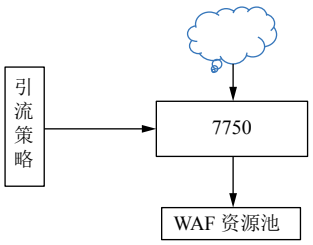

图 7 常规 SDN 引流

如图 7 的流程图所示, 首先用户通过平台控制平面的操作把引流信息通过 NETCONF 下达给 7750 流量牵引的命令,其次从流量层面来看首先流量通过 7750 进行牵引, 结合控制层面来看, 整体的 SDN 的东西向引流如下:

1) 公网访问防护 IP 时, 经过 7750 后, 路由到 WAF, 此时的流量过程为源目地址为: 客户端 IP——WAF.

2) 软 WAF 对流量进行检测, 合规请求通行, 并对源地址进行转换, 此过程源目地址为: Nat_WAF——业务网络服务器 IP.

4) 业务网络服务器将响应内容发送给软 WAF, 此过程源目地址为: 业务网络服务器 IP——Nat_WAF.

5) 软 WAF 收到业务网络服务器的响应后, 转发响应内容给客户端.

7750 构成了业务侧的核心, 防护策略、流量牵引只能通过 7750 串行下达, 无法并发的进行流量的牵引. 导致防护吞吐量较低.

4.2 改造 WAF 引流拓扑

在高性能 SDN 并发引流的改造如图 8，具体思路提出如下.

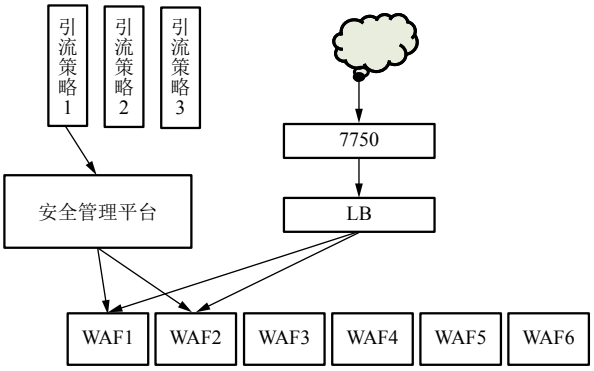

图 8 SDN 引流改造

1) 以 6 台 WAF 为. 他们按照 hash 映射算法与平台映射.

2) 通过安全管理平台下发实际的防护策略直接到设备 WAF1, WAF2 上此时策略到 WAF1、WAF2 上的 IP 为真实 IP.

3) SDN 将保护流量直接牵引到 LB.

4) 此时 LB 和平台采用与 1) 一致的 hash 映射算法牵引到目的 WAF 设备, 牵引地址为 WAF1 和 WAF2 的共同的高可用地址 VIP.

分析结构: 此时的拓扑接口控制防护策略从上图的左侧通过安全管理平台直接进行下发, 通过平台算法映射下发到 WAF 设备, 而承载流量通过有 7750 的 SDN 网络新加 LB 并与平台相同映射, 实现策略对应的 WAF 实现策略与流量承载分离.

总结: 1) 改造后使得用户侧防护策略可以绕过 7750 直接通过平台映射到对应设备, 使得控制端可以并发调用防护. 2) 7750 不用关心具体的引流目标 WAF, 只需把流量引入 LB, 由 LB 采取对应控制端引流映射 WAF, 实现对应策略的流量牵引.

5 试点实验效果

本章实验在中国移动某省公司公有云进行试点测试, 分别实验 (采用流量监测提升和拓扑改造提升) 高性能 WAF 方案比业界传统方案的流量监测防护效率和流量吞吐量.

5.1 实验流量监测效率

测试环境 1 搭建: WAF 流量检测端与流量业务发送端直连, 对流量检测端进实验测试对比分析, 对象为 1: 高性能 WAF 方案和 2: 传统 WAF 防护方案. 测试模型如图 9.

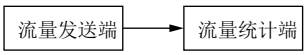

图 9 测试模型

测试内容为对 0.2 s 后开始同时分别对两组 WAF 模块分别发送 500 mb/s 的流量来考察观测对象 1: 在测试时间高性能方案的流量监测结果. 2: 常规方案的流量监测结果. 两组的时间段都一致, 发送端和接收端的测试时间也相同.

1 和 2 对象测试结果如图 10.

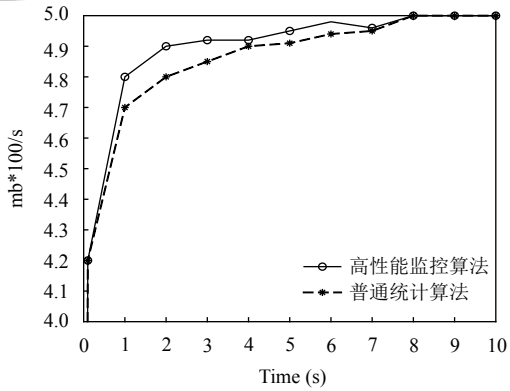

图 10 流量监测效率对比

实验仿真测试结果验证思路为验证流量统计和实际流量偏移量, w 为统计时间. 其中为 $s(w)$ 高性能监控算法监控统计流量, $u(w)$ 为常规算法监控统计流量. $\theta 1$、$\theta 2$ 为对应算法偏差量.

$$\theta 1 = (5 - s(\omega))^2 \tag{1}$$

$$\theta 2 = (5 - u(\omega))^2 \tag{2}$$

实验 1 结果分析:

1) 流量发送端, 向 WAF 系统发送需要防护监测的流量. 在时间在 0.2 s 时刻, 发送流量由 0 b/s 突发增加到 500 mb/s.

2) 流量统计端, 为 WAF 系统内防护流量统计, 如图 11, 采用改造流量监测统计算法的高性能 WAF 系统, 面对突发数据压力, 按照 3.4 自适应算法预期, 迅速自适应增加处理能力, 在 1 s 时刻, 就监控解析了 480 mb/s 以上的流量.

3) 对比传统 WAF 系统, 其到 3.2 s 时刻才监控解析了 480 mb/s 以上的流量. 在 $w \in (0-1)$ 偏差的监测数

据包因为传统方案无动态自增处理能力机制而大量丢包. 1 s 时刻手动增加传统方案监测资源能力, 才慢慢在 3.2 s 时刻监测足够数据.

4) 1)–3) 分析结合仿真计算结论式 (1) 和式 (2), 得到采用改造流量监测方案的高性能 WAF 方案比传统 WAF 系统的流量监测丢包率更少, $\theta 1$小于$\theta 2$更高效贴合实际流量的承载. 因而高性能 WAF 方案的防护效率更高.

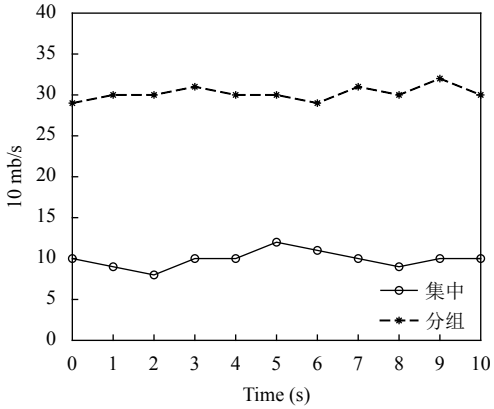

图 11 防护吞吐量对比

5.2 实验防护吞吐量

实验 2 设计: 对象 1、2 同时对公有云环境内的 3 台云主机按照相同策略进行 WAF 防护.

实验对象为 1: 高性能 WAF 方案, 2: 传统 WAF 防护方案, 单台业务访问流量访问为 10 mb/s. 实验测试对象为检测 WAF 防护系统池的防护吞吐量.

时间w选取说明, 单台主机策略的 WAF 防护系统的调度启动周期为 10 s 以上, 启动后 WAF 系统有吞吐流量可以统计. 实验选取第一个启动周期中的 10 s 时间段作为统计周期来进行统计. $w \in (0–10)$.

实验 2 结果分析:

1) 传统 WAF 防护方案在第一个启动周期 10 s 内, $w \in (0–10)$顺序启动了一台主机的流量防护, 而其他主机防护策略还在排队, 统计周期内整个传统 WAF 方案在 10 mb 左右的防护流量.

2) 高性能的 WAF 方通过改造引流拓扑, 策略与引流承载分离, 测试结果实现可并发的防护, 如图在 $w \in (0–10)$, 3 台的防护流量全部牵引到位.

3) 结合 1、2 得到采用高性能并发拓扑的高性能的 WAF 方案, 可以实现 WAF 流量牵引的并发调度, 在第一个调度启动周期后就可以实现并发调度 3 台主机的并发流量防护, 达到 30 mb 左右, 因而高性能 WAF 方案的实现了无任务排队的并发高吞吐量防护.

6 总结

通过改造流量监测方案在流量监测改造上设计的处理步骤自适应机制算法, 在公有云实施测试中有效实现了下游网络处理能力自适应匹配, 减少了监测流量的丢包, 提高了 WAF 流量监测效率.

通过改造 WAF 防护拓扑的安全方案: 新加平台策略映射, 新加 LB 对应引流, 有效绕过传统方案的交换机 7750 串行处理核心的问题, 通过平台端直接映射策略到设备, 网络侧新加 LB 将对应映射策略引流. 实现 WAF 防护控制与承载分离, 由此公有云实施测试中, 证明了可并发用户调度实现方案高吞吐的提升.

参考文献

1 王峰, 张骁, 许源, 等. Web 应用防火墙的国内现状与发展建议. 中国信息安全, 2016, (12): 80–83. [doi: 10.3969/j.issn.1674-7844.2016.12.033]

2 王国峰, 刘川意, 潘鹤中, 等. 云计算模式内部威胁综述. 计算机学报, 2017, 40(2): 296–316. [doi: 10.11897/SP.J.1016.2017.00296]

3 江国龙. 东西向流量牵引方案小结. http://blog.nsfocus.net/east-west-Flow-sum/. [2018-03-10].

4 Awan II, Shah N, Imran M, *et al*. WITHDRAWN: An improved mechanism for flow rule installation in-band SDN. Journal of Systems Architecture, 2019, 96: 32–51. [doi: 10.1016/j.sysarc.2019.03.002]

5 张永铮, 肖军, 云晓春, 等. DDoS 攻击检测和控制方法. 软件学报, 2012, 23(8): 2058–2072.

6 Wang J, Yang XL, Zhang M, *et al*. HTTP-SoLDiER: An HTTP-flooding attack detection scheme with the large deviation principle. SCIENCE CHINA Information Sciences, 2014, 57(10): 1–15.

7 何丹. 一种层次化多阈值 DDoS 防御模型研究[硕士学位论文]. 南京: 南京邮电大学, 2014.

8 柳林, 周建涛. 软件定义网络控制平面的研究综述. 计算机科学, 2017, 44(2): 75–81. [doi: 10.11896/j.issn.1002-137X.2017.02.009]

9 王涛, 陈鸿昶, 程国振. 软件定义网络及安全防御技术研究. 通信学报, 2017, 38(11): 133–160. [doi: 10.11959/j.issn.1000-436x.2017221]

10 Dayal N, Maity P, Srivastava S, *et al*. Research trends in security and DDoS in SDN. Security and Communication Networks, 2016, 9(18): 6386–6411. [doi: 10.1002/sec.1759]

11 张恒, 蔡志平, 李阳. SDN 网络测量技术综述. 中国科学: 信息科学, 2018, 48(3): 293–314.

12 王鹃, 刘世辉, 文茹, 等. 基于 OpenFlow 的 SDN 状态防火墙. 计算机工程与应用, 2018, 54(15): 84–90. [doi: 10.3778/j.issn.1002-8331.1703-0411]