**自动化线上模拟测试平台**

**一、背景**

1、目前测试环境请求数据单一，防护配置复杂度不够，造成测试覆盖度不够。由于线上请求数据复杂，每个域名的配置复杂并且多样性，往往测试后的版本部署线上发生异常。

2、压测数据单一，无法正真反映机器的性能

3、规则新增的时候，对规则测试的数据比较单一，可能会引起误拦、CPU跑高的风险。

需求

模拟线上请求流量，测试的waf 配置和线上配置一致。发布前对waf的全部域名进行测试，统计异常状态，判断系统是否正常。当下发新规则前，需要先下发到测试平台，平台进行压测，判断是否误拦和CPU变化情况。

**二、整体方案**



1. 线上真实流量收集，还原并下发到测试服务器。
2. 控制服务器发生测试指令。
3. 压测机器控制模块根据具体模式压测机器进行流量回放测试。
4. Waf控制模块根据具体模式选择对应的配置，启动waf。
5. waf统计模块根据压测模式对日志、性能数据分析统计。
6. 收集压测机器和waf统计模块的分析数据，发送到控制服务器上。
7. **具体实现**

3.1线上真实流量收集

线上多台父tcpdump

Nginx lua模块

Tcpcopy回放

Pcap数据包

Request.data

解析请求并一定格式保存

压测机器3

压测机器2

压测机器1

Request.data格式：

{

[

{

“url”:[www.test.com/?test=1](http://www.test.com/?test=1),

“method”:”GET/POST”,

“header”:{

“host”:xxxx,

“user-agent”:xxxx

…….

}

“body”:base64(实际body)

}

]

}

3.2流量回放测试

Manager server

测试指令（选择模式）

压测机器1

Waf环境

测试模式：

1. 质量测试模式，调用压测机器，循环压测所有域名。（压力cpu达到50%左右。）
2. 压测模式，调用所有压测机器，并加大并发包进程数，随机压测域名（cpu达到100%，内存指标，qps指标，错误状态码指标）
3. 域名配置上限模式(逐步增加域名数，同时压测输出监控内容，直到机器指标达到设定值内存)
4. 单条规则测试模式（需要去掉全局黑名单和自定义黑名单，只保留单条待测试规则，避免其他规则编译进入引擎影响匹配效率）
5. 频繁reload模式（设置reload间隔时间，然后压测，观察各项指标是否异常）
6. 频繁restart模式（设置restart间隔时间，然后压测，观察各项指标是否异常）
7. 频繁动态加载模式（不停下发动态加载，观察请求是否正常及进程内存变化）
8. 单功能测试模式（关闭其他功能，开启单个功能进行压测，观察性能指标变化）

3.3控制模块



3.2统计分析模块

模式一（目前实现模式一，其他模式后续版本实现）：

Waf端分析过程



步骤1、稳定版本进行压测，建立标准参考基线指标

步骤2、替换测试版本进行压测，获取实际指标

压测机器数据分析统计：

Qps，整体压测时间，发送请求数，成功请求数（日志记录发送失败请求）。

waf数据分析统计：

性能指标：cpu和内存，每分钟记录一个值（详细的值（进程号.cpu/men），最大值，最小值，平均值）

状态码指标：所有状态码数量和基线状态码对比，如果偏差则产生告警。

记录所有错误状态码400,403,408,499,500,502,503日志，文件格式：域名.时间戳.版本号。

3.3整体报告展示

收集压测机器和waf统计模块的分析数据，发送到控制服务器上