北京大学基于WAF服务的网站安全探索

李若淼

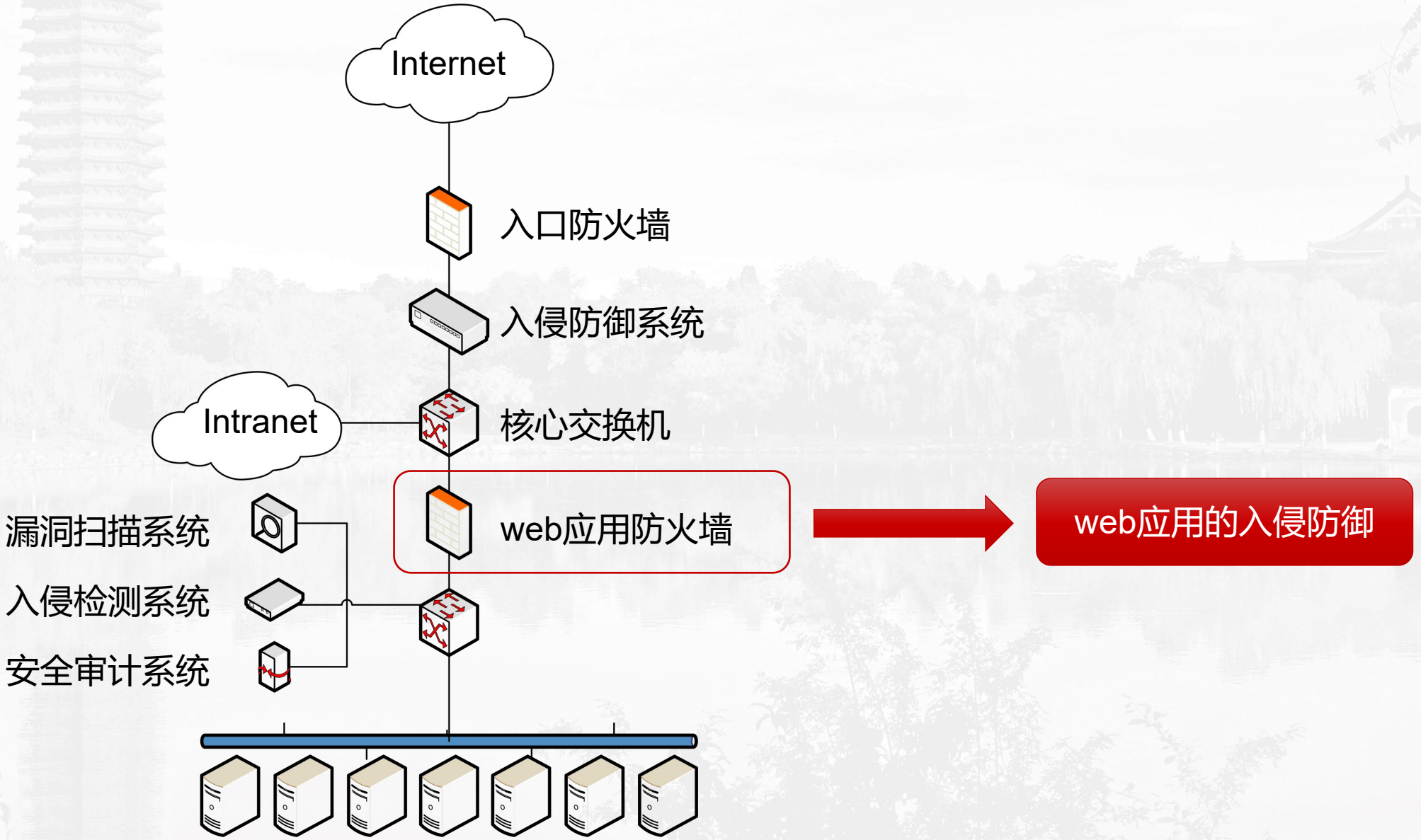
北京大学计算中心

2018-10-20

提纲

- 问题和现状
- 需求和目标
- 设计思路
- 系统介绍
- 运行情况
- 下一步工作

问题和现状 —— 问题


Internet
入口防火墙
入侵防御系统
Intranet
核心交换机
漏洞扫描系统
web应用防火墙
入侵检测系统
安全审计系统
web应用的入侵防御

问题和现状 —— 现状

- 从网站数量来看，北京大学已经有1000多个网站，并且在持续增加中
- 从网站所属方看，校内各个部门、组织、团体甚至个人都有网站
- 从网站分布来看，服务器放置在学校各楼各房间，IP遍布各个全校网段

问题和现状 —— 现状

- 网站建设水平难以得到保障
- 网站维护运维难以得到足够重视

问题和现状 —— 现状

- 2017年我国境内被篡改的网站数超过了2万个，较2016年增长了约20%；
- 出现众多针对高校的web应用攻击

问题和现状 —— 现状

- 现状总结：
  1. 网站数量多
  2. 网站管理难
  3. 网站威胁大

需求和目标

大规模

需要对全校网站进行集中管理，具备大规模网站防护能力

细粒度

为每个网站都提供应用防护和个性化配置管理，具备以网站为单位的细粒度配置能力

稳定高效

保证网站的正常访问，对用户透明，能够稳定高效运行

易部署

最小化对现有系统的影响，能够不改变现有网络结构，不改变网站服务器配置

易管理

提供网站管理员易于接受的管理模式，具备灵活管理的能力

可能的解决方案

加强网站安全管理

- 优点：能够从根本上解除安全隐患
- 缺点：客观困难太多

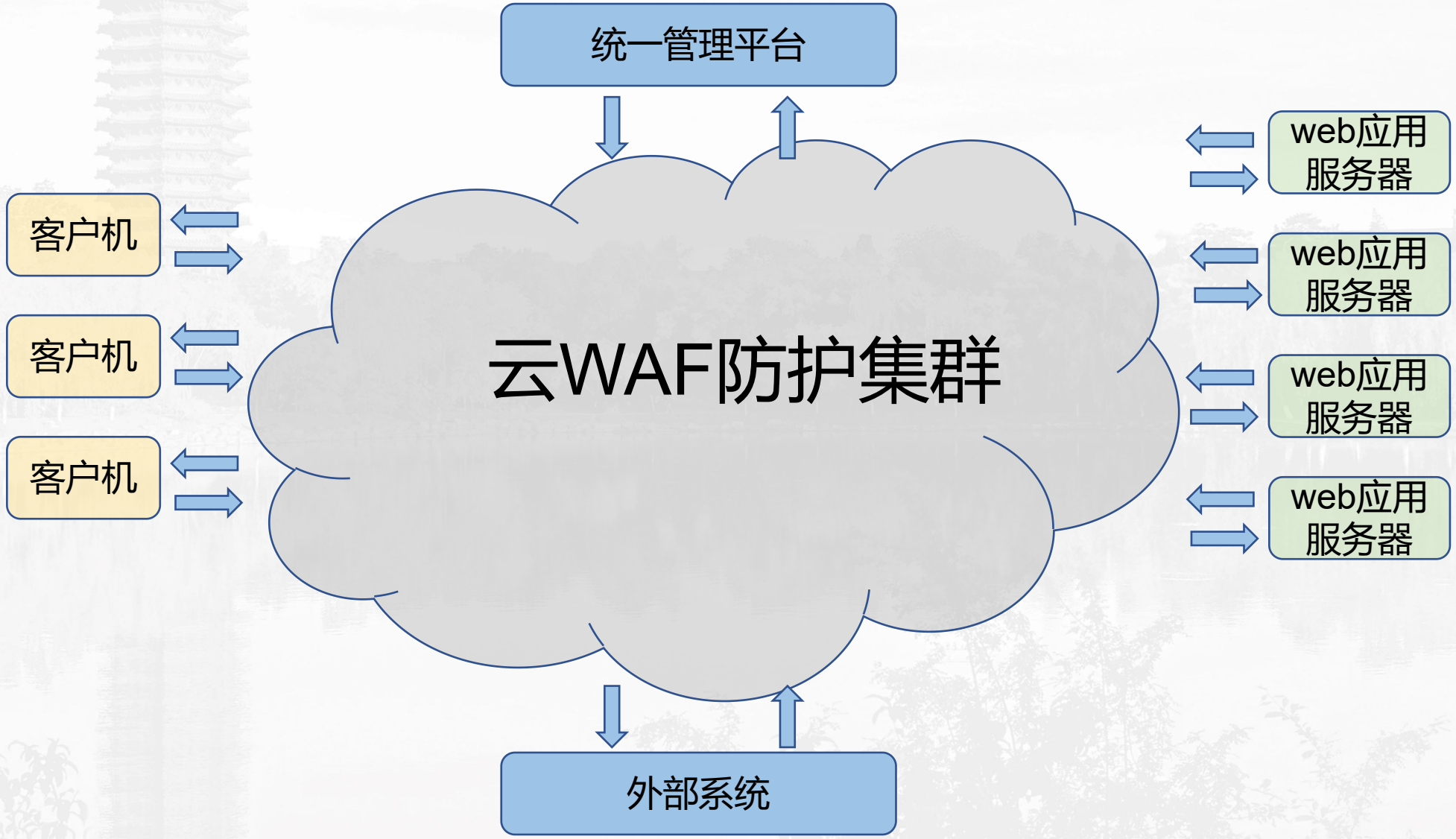
采用商用WAF系统

- 优点：成熟的防护能力
- 缺点：有一定局限性

自建应用防护平台

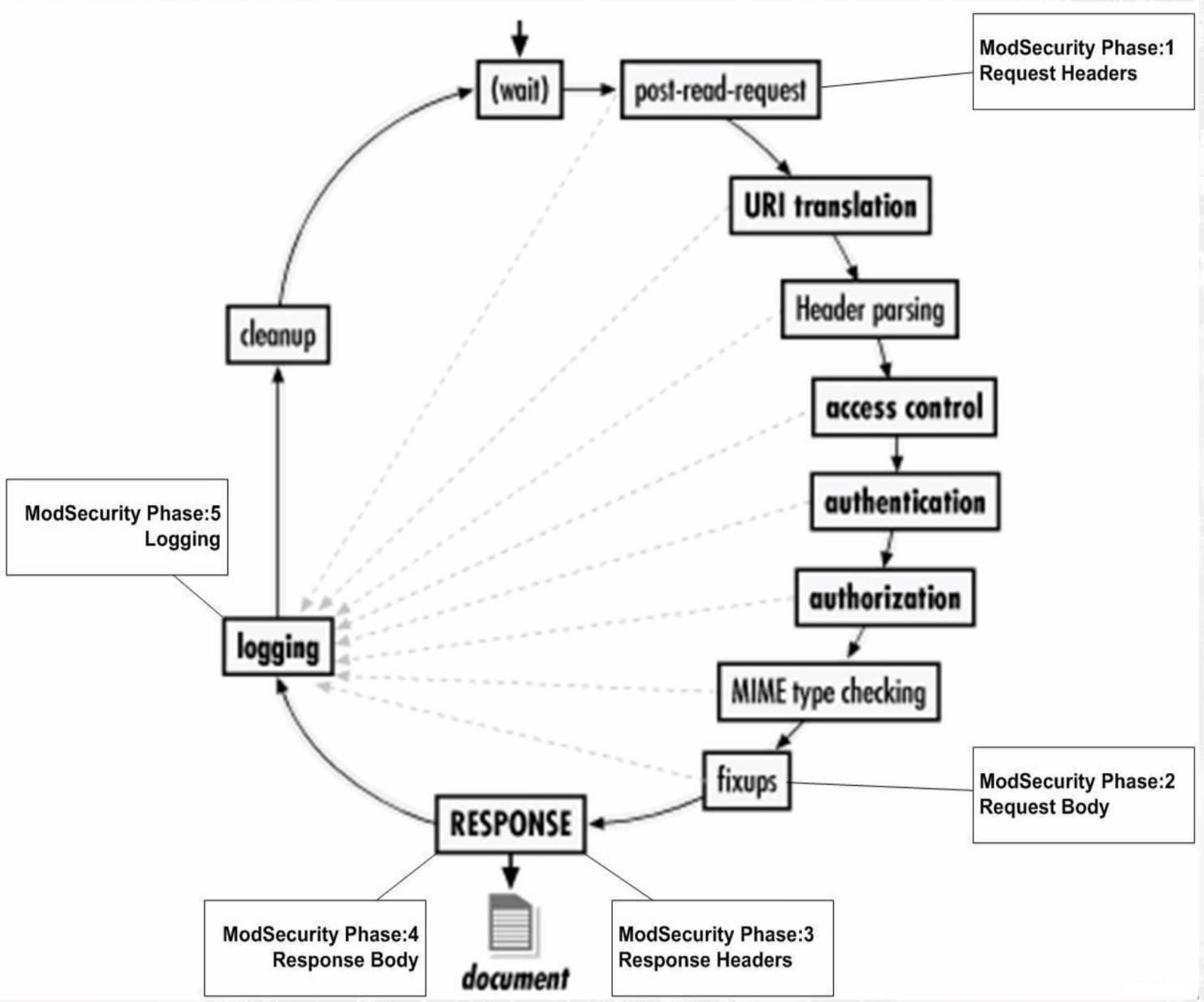
- 优点：自主可控
- 缺点：使用风险

设计思路 —— 控制平面与数据平面分离

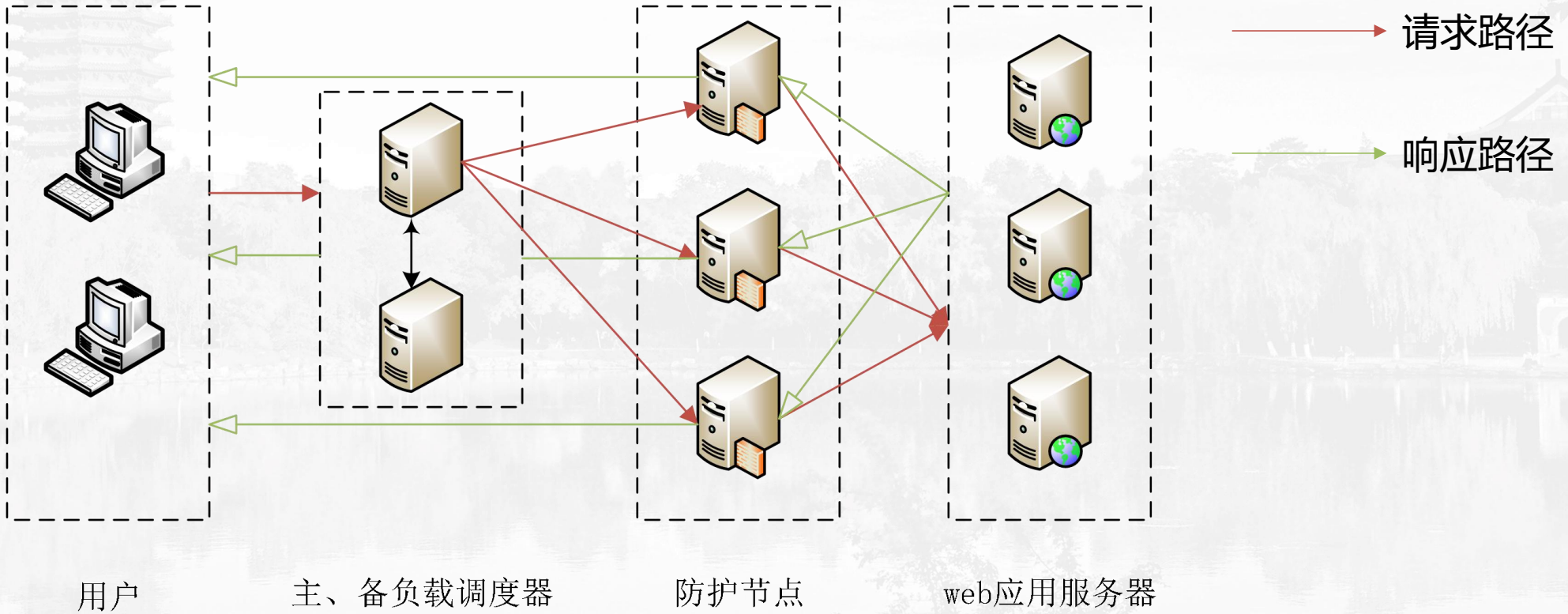


设计思路 —— 基于ModSecurity的应用防护服务

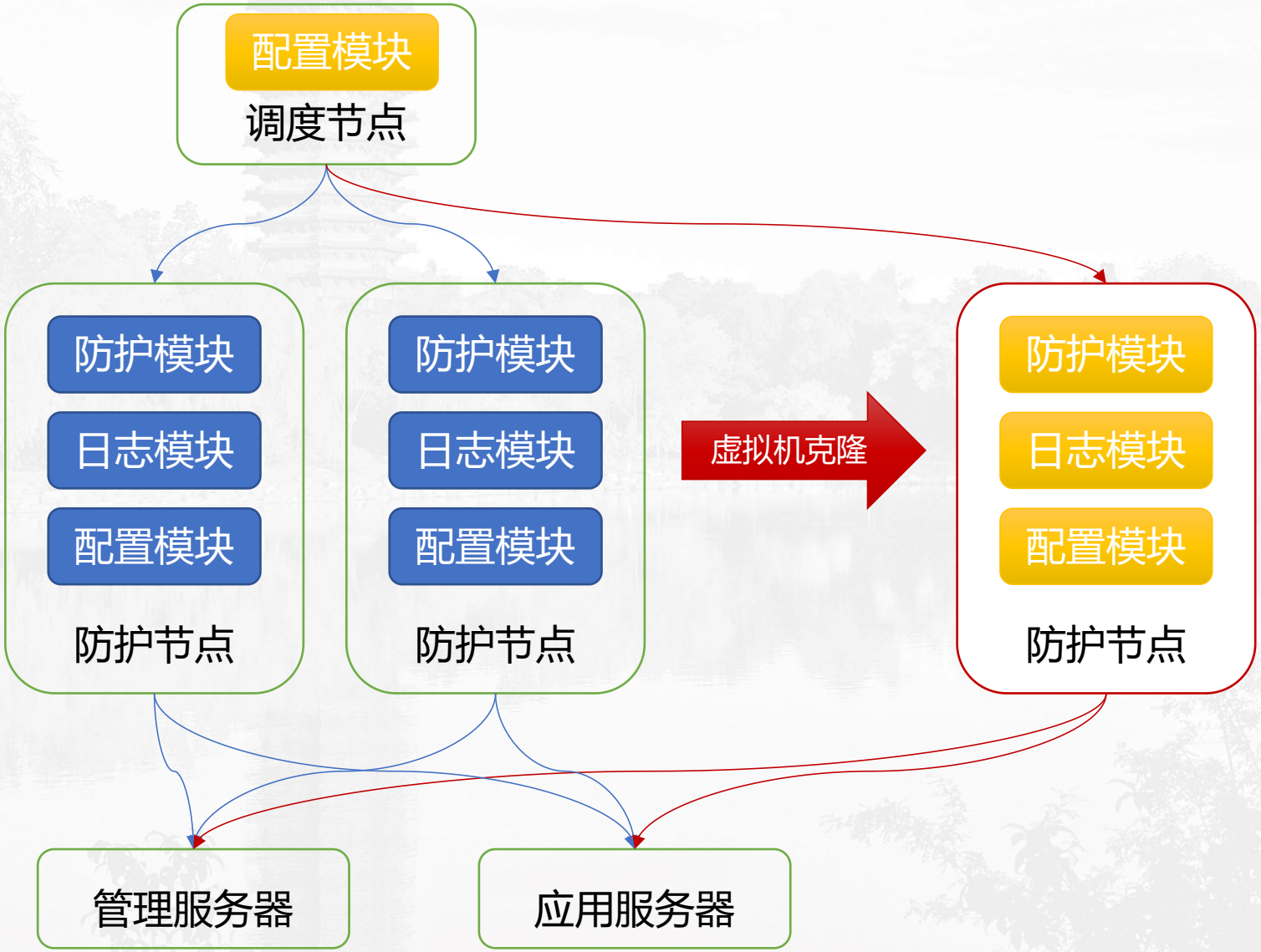
- ModSecurity主要功能
  - 解析
  - 缓存
  - 日志
  - 规则引擎
- ModSecurity其他特点：
  1. 开源免费
  2. 稳定成熟
  3. 配置灵活



设计思路 —— 通过LVS负载均衡提高可用性

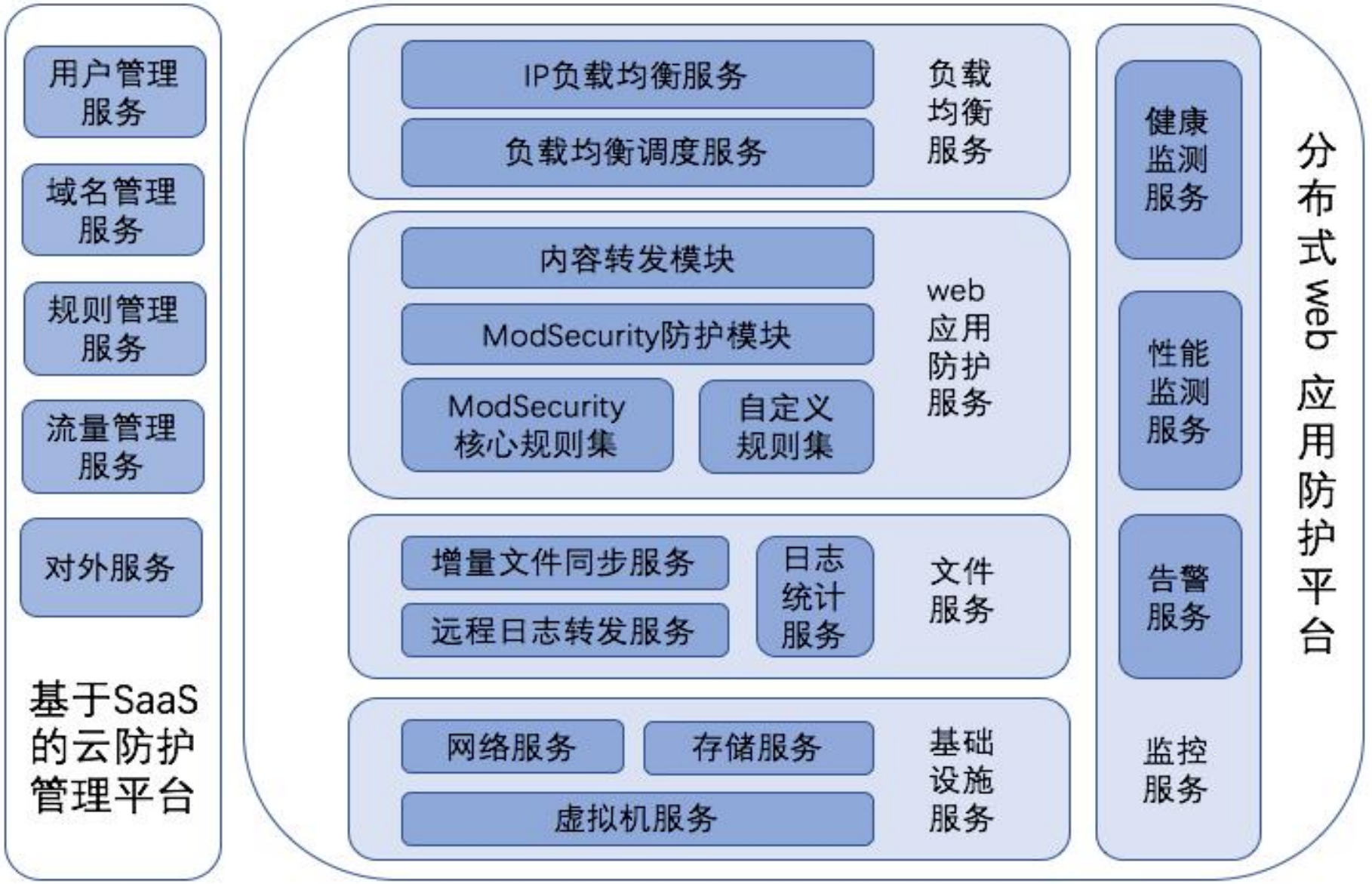


设计思路 —— 基于虚拟机复制的扩展能力

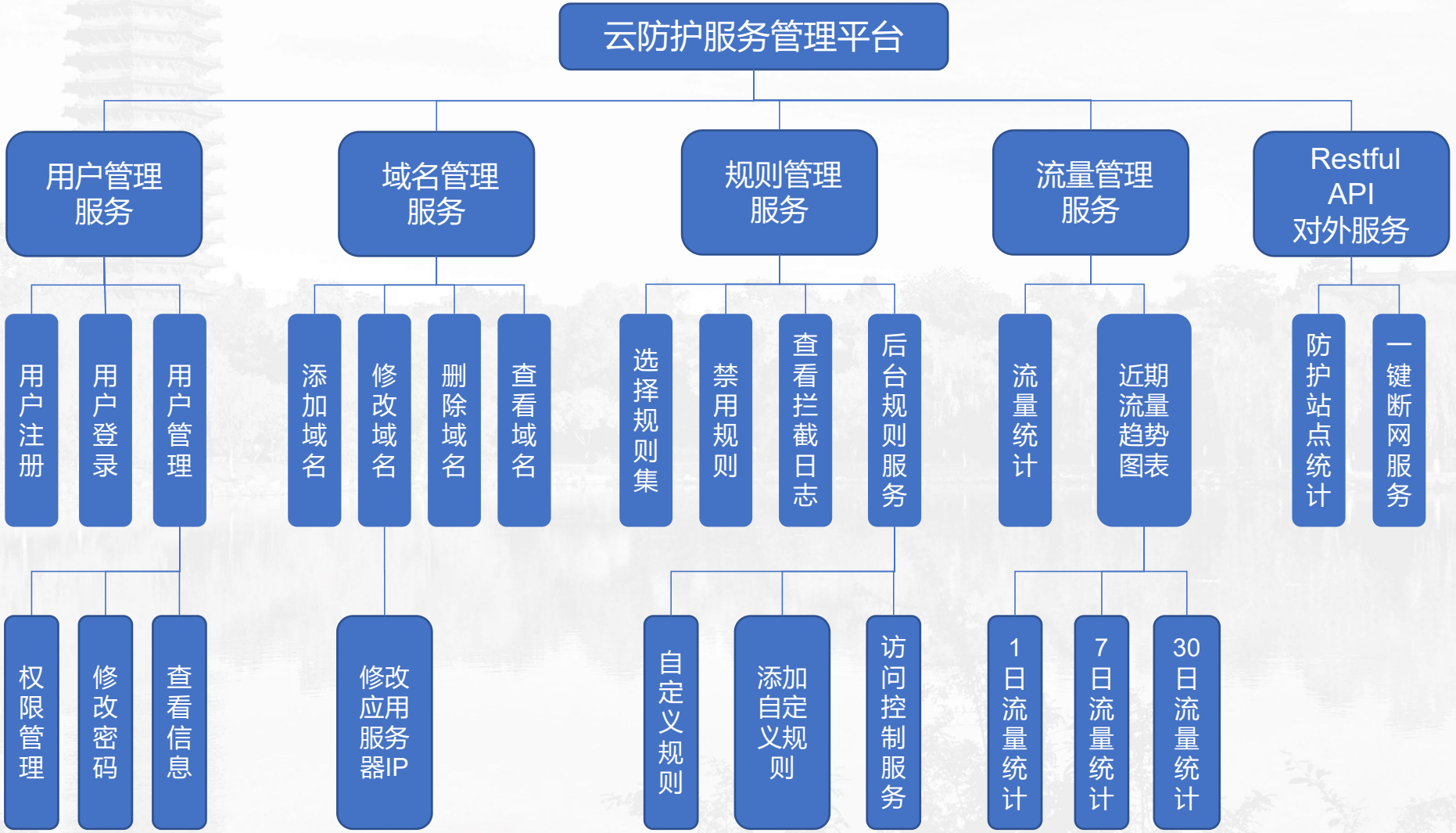


设计思路 —— 基于SAAS的管理服务

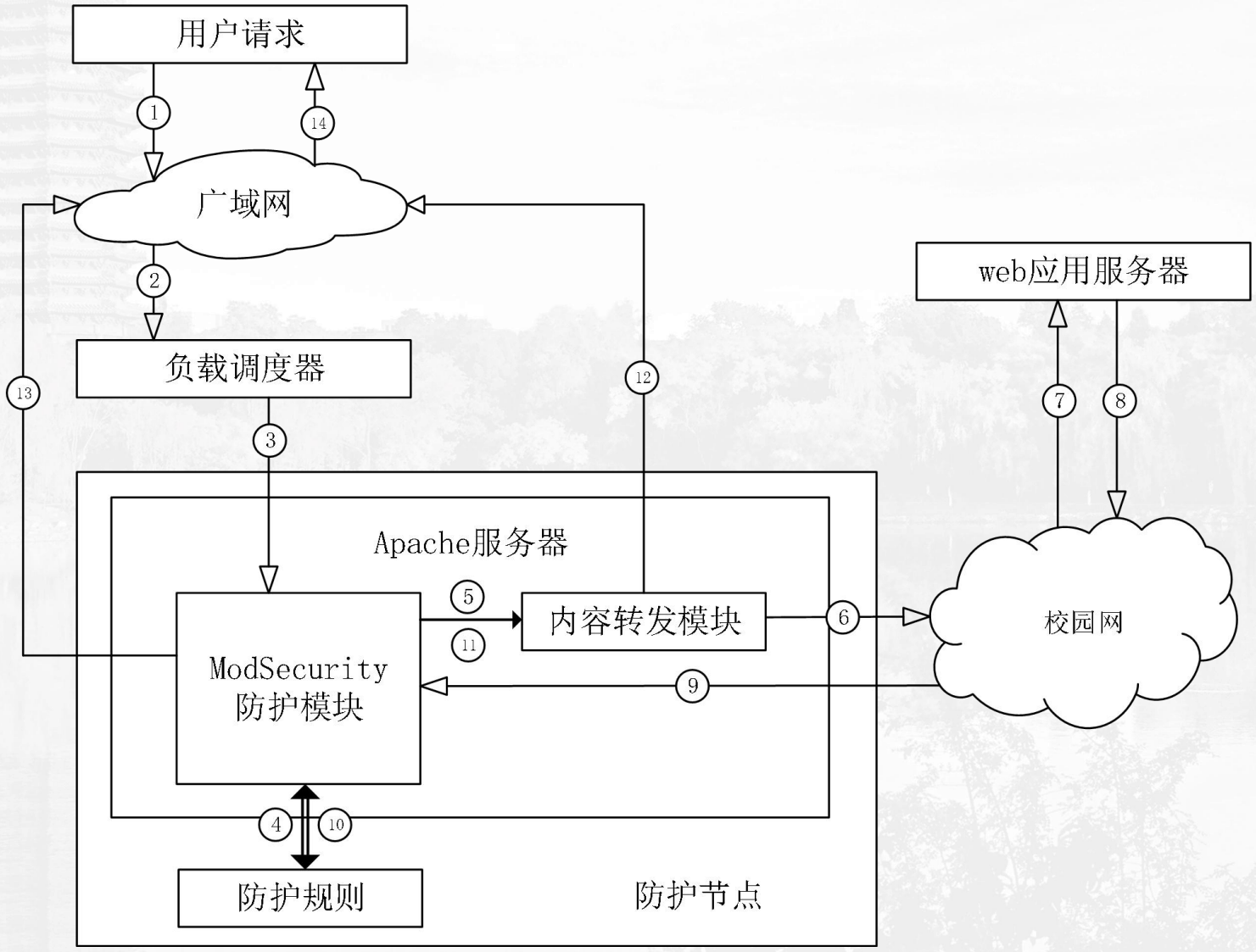
系统介绍 —— 系统服务架构


用户管理服务
域名管理服务
规则管理服务
流量管理服务
对外服务
基于SaaS的云防护管理平台
IP负载均衡服务
负载均衡调度服务
负载均衡服务
内容转发模块
ModSecurity防护模块
ModSecurity核心规则集
自定义规则集
web应用防护服务
增量文件同步服务
远程日志转发服务
日志统计服务
文件服务
网络服务
存储服务
虚拟机服务
基础设施服务
健康监测服务
性能监测服务
告警服务
监控服务
分布式web应用防护平台

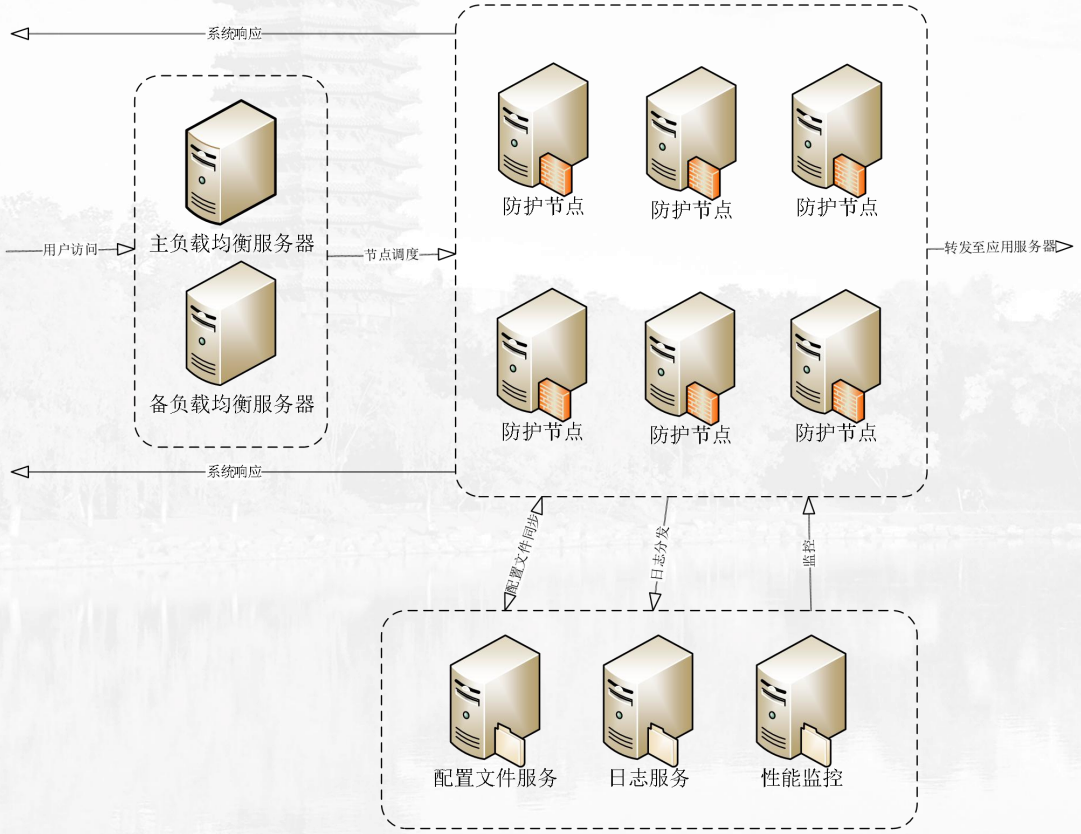
系统介绍 —— 管理平台功能


云防护服务管理平台
用户管理服务
域名管理服务
规则管理服务
流量管理服务
Restful API 对外服务
用户注册
用户登录
用户管理
添加域名
修改域名
删除域名
查看域名
选择规则集
禁用规则
查看拦截日志
后台规则服务
流量统计
近期流量趋势图表
防护站点统计
一键断网服务
权限管理
修改密码
查看信息
修改应用服务器IP
自定义规则
添加自定义规则
访问控制服务
1日流量统计
7日流量统计
30日流量统计

系统介绍 —— 用户请求生命周期

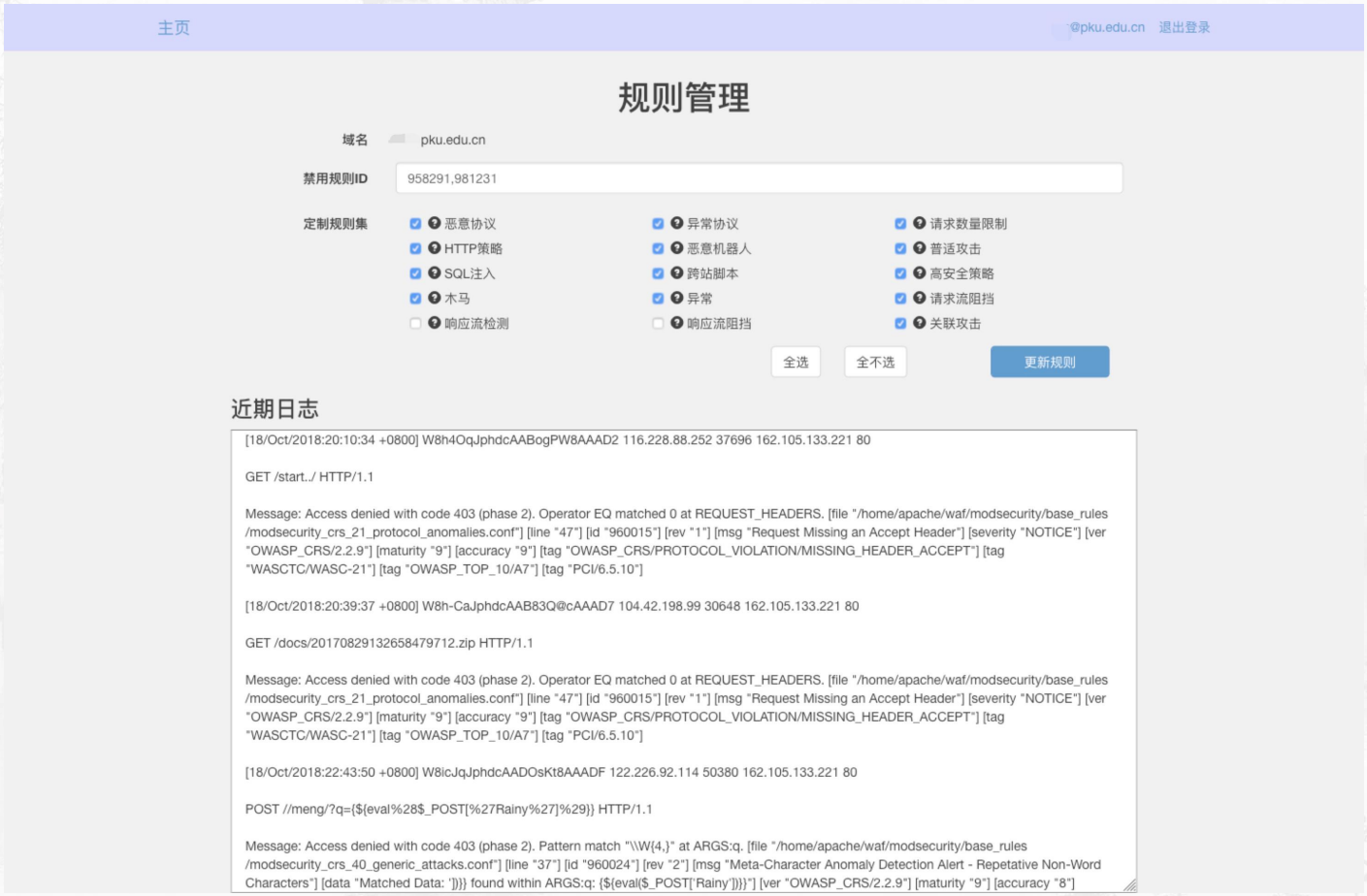


运行情况 —— 部署方式



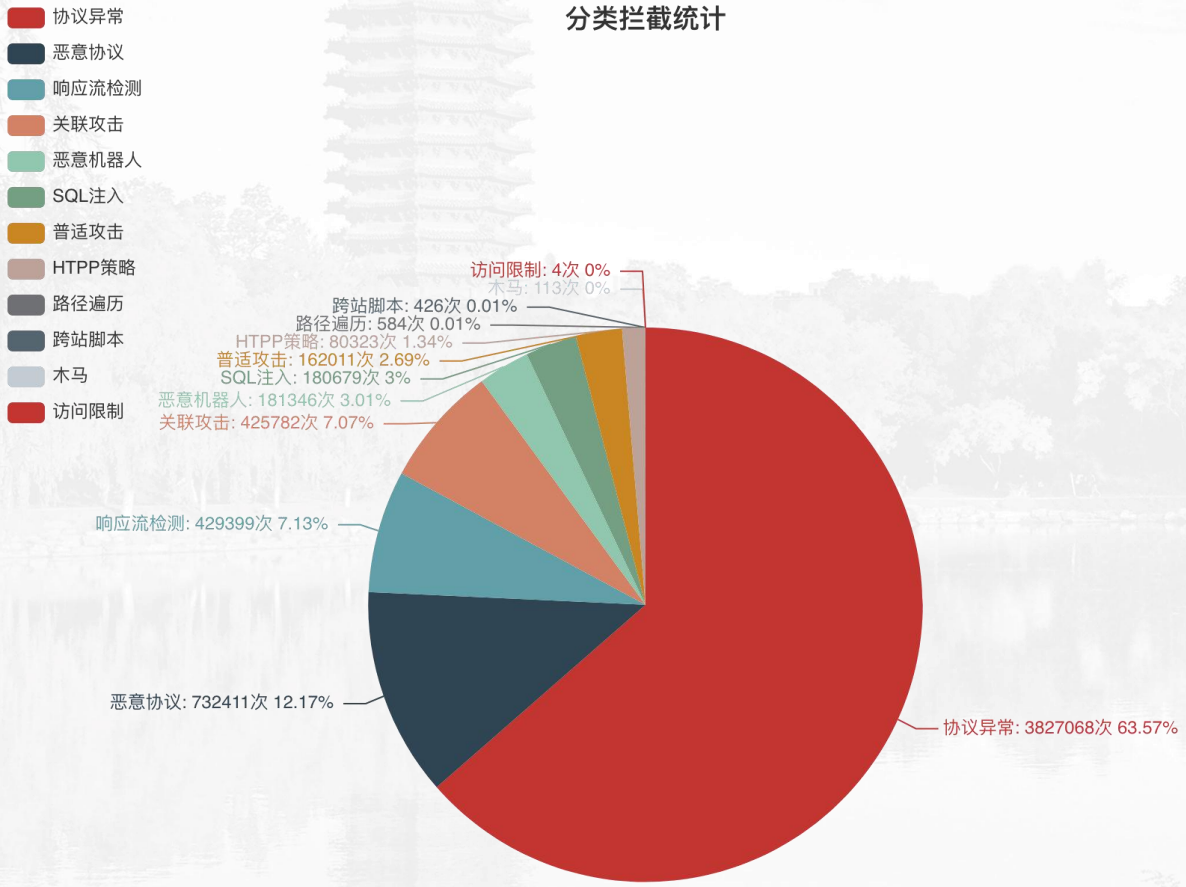
服务器	数量	核数	内存
管理服务器	1	4	4GB
负载调度器	2	2	2GB
防护节点	5	4	16GB
备用节点	1	4	16GB
日志服务器	1	4	4GB
数据库服务器	1	4	4GB

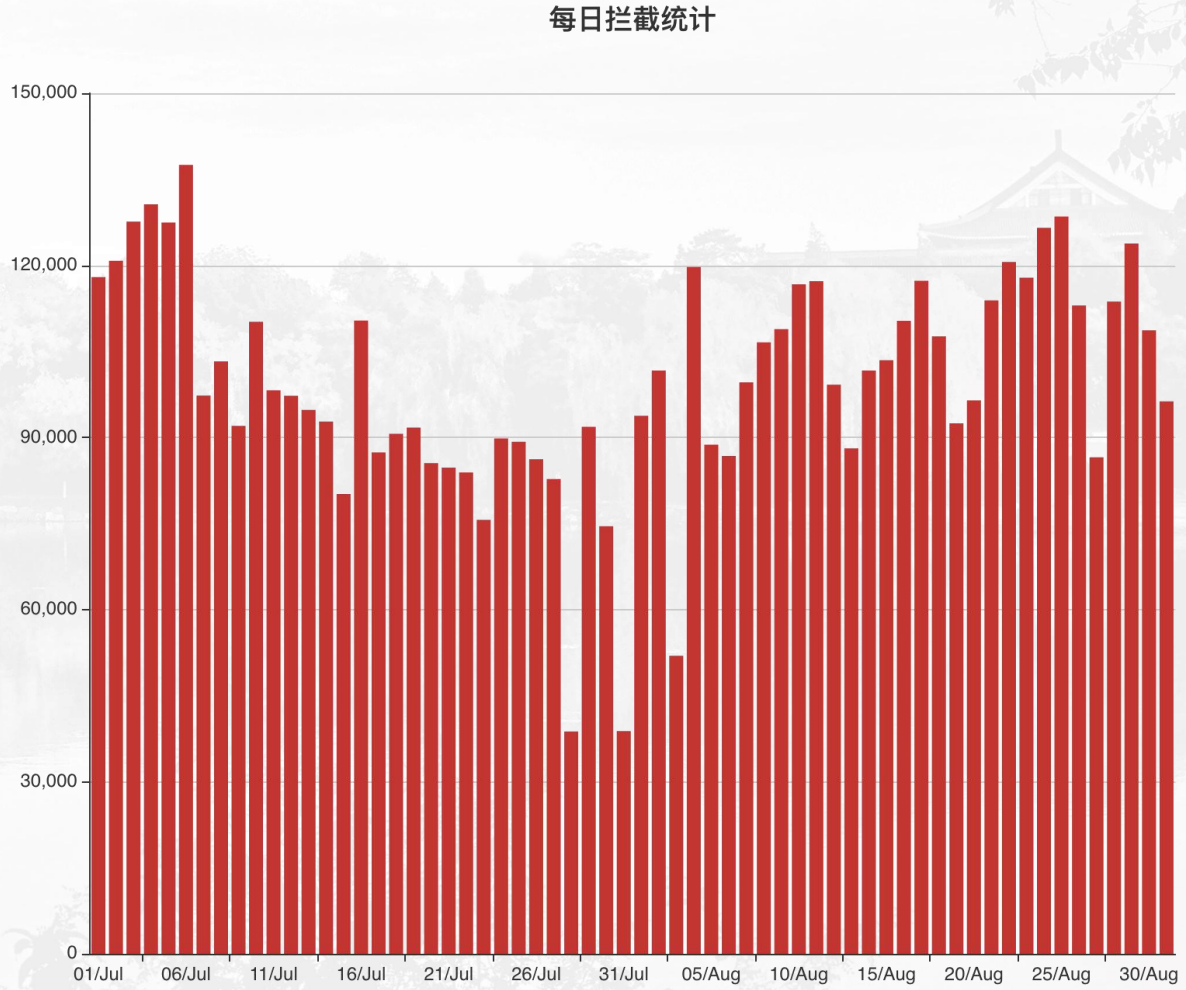
运行情况 —— 防护规则配置


主页
@pku.edu.cn 退出登录
规则管理
域名
pku.edu.cn
禁用规则ID
958291,981231
定制规则集
恶意协议
HTTP策略
SQL注入
木马
响应流检测
异常协议
恶意机器人
跨站脚本
异常
响应流阻挡
请求数量限制
普适攻击
高安全策略
请求流阻挡
关联攻击
全选
全不选
更新规则
近期日志
[18/Oct/2018:20:10:34 +0800] W8h4OqJphdcAABogPW8AAAD2 116.228.88.252 37696 162.105.133.221 80
GET /start../ HTTP/1.1
Message: Access denied with code 403 (phase 2). Operator EQ matched 0 at REQUEST_HEADERS. [file "/home/apache/waf/modsecurity/base_rules /modsecurity_crs_21_protocol_anomalies.conf"] [line "47"] [id "960015"] [rev "1"] [msg "Request Missing an Accept Header"] [severity "NOTICE"] [ver "OWASP_CRS/2.2.9"] [maturity "9"] [accuracy "9"] [tag "OWASP_CRS/PROTOCOL_VIOLATION/MISSING_HEADER_ACCEPT"] [tag "WASCTC/WASC-21"] [tag "OWASP_TOP_10/A7"] [tag "PCI/6.5.10"]
[18/Oct/2018:20:39:37 +0800] W8h-CaJphdcAAB83Q@cAAAD7 104.42.198.99 30648 162.105.133.221 80
GET /docs/20170829132658479712.zip HTTP/1.1
Message: Access denied with code 403 (phase 2). Operator EQ matched 0 at REQUEST_HEADERS. [file "/home/apache/waf/modsecurity/base_rules /modsecurity_crs_21_protocol_anomalies.conf"] [line "47"] [id "960015"] [rev "1"] [msg "Request Missing an Accept Header"] [severity "NOTICE"] [ver "OWASP_CRS/2.2.9"] [maturity "9"] [accuracy "9"] [tag "OWASP_CRS/PROTOCOL_VIOLATION/MISSING_HEADER_ACCEPT"] [tag "WASCTC/WASC-21"] [tag "OWASP_TOP_10/A7"] [tag "PCI/6.5.10"]
[18/Oct/2018:22:43:50 +0800] W8icJqJphdcAADOsKt8AAADF 122.226.92.114 50380 162.105.133.221 80
POST //meng/?q=${eval%28$_POST[%27Rainy%27]%29} HTTP/1.1
Message: Access denied with code 403 (phase 2). Pattern match "\\W{4,}" at ARGS:q. [file "/home/apache/waf/modsecurity/base_rules /modsecurity_crs_40_generic_attacks.conf"] [line "37"] [id "960024"] [rev "2"] [msg "Meta-Character Anomaly Detection Alert - Repetative Non-Word Characters"] [data "Matched Data: '])}} found within ARGS:q: {${eval($_POST['Rainy'])}}"] [ver "OWASP_CRS/2.2.9"] [maturity "9"] [accuracy "8"]


配置web站点
访问站点
没有出现访问被阻挡的情况
出现正常访问被阻挡
查看日志记录，找到对应规则
填写禁用对应规则
等待防护节点更新配置文件

运行情况 —— 数据统计


分类拦截统计
协议异常
恶意协议
响应流检测
关联攻击
恶意机器人
SQL注入
普适攻击
HTPP策略
路径遍历
跨站脚本
木马
访问限制
访问限制: 4次 0%
木马: 113次 0%
跨站脚本: 426次 0.01%
路径遍历: 584次 0.01%
HTPP策略: 80323次 1.34%
普适攻击: 162011次 2.69%
SQL注入: 180679次 3%
恶意机器人: 181346次 3.01%
关联攻击: 425782次 7.07%
响应流检测: 429399次 7.13%
恶意协议: 732411次 12.17%
协议异常: 3827068次 63.57%


每日拦截统计
150,000
120,000
90,000
60,000
30,000
0
01/Jul
06/Jul
11/Jul
16/Jul
21/Jul
26/Jul
31/Jul
05/Aug
10/Aug
15/Aug
20/Aug
25/Aug
30/Aug

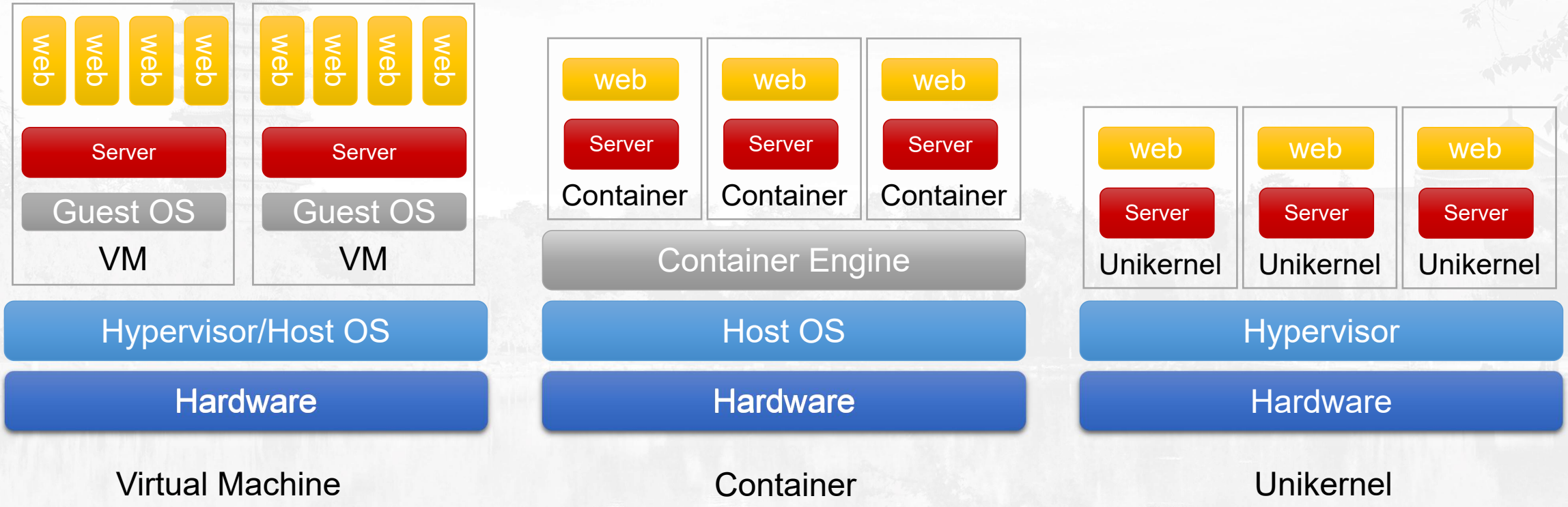
运行情况 —— 基于平台的其他功能

- 一键断网服务
- 请求分发服务
- 日志分析
- 流量记录

下一步工作

- 提高云WAF防护平台的应用安全防护能力；
- 继续增加以云WAF防护平台为中心的网站管理功能，提供更多服务；
- 进一步提高云WAF防护平台的处理能力；

下一步工作



	Virtual Machine	Container	Unikernel
资源消耗	大	小	很小
隔离性	好	不好	好
伸缩性	不好	好	很好

谢谢大家！