毕设开题答辩

设计题目：塔菲网络服务防御系统的开发

东北林业大学计算机与控制工程学院

导师：王波

答辩人：孙雷(20级软件工程2班)

2023

CLINESE

目录

CONTENTS

01 选题背景及内容

02 详细功能

03 技术栈及实现原理

04 可能遇到的问题和解决方案

PART
ONE

01

选题背景及内容

选题背景

中国政府对网络安全重视程度

2015年

《中华人民共和国国家安全法》

2016年

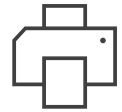
护网行动：由公安机关统一组织的"网络安全实战攻防演习

2017年

《中华人民共和国数据安全法》

2021年上半年

《中华人民共和国数据安全法》



2021年下半年

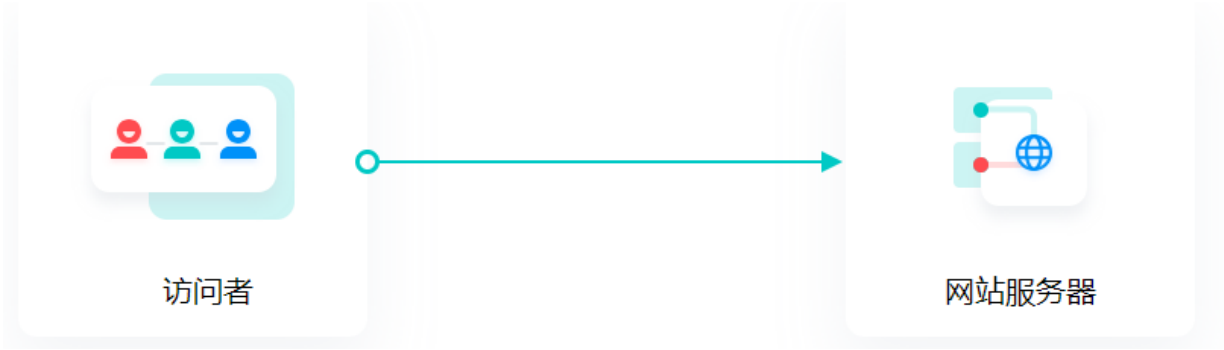
《中华人民共和国个人信息保护法》

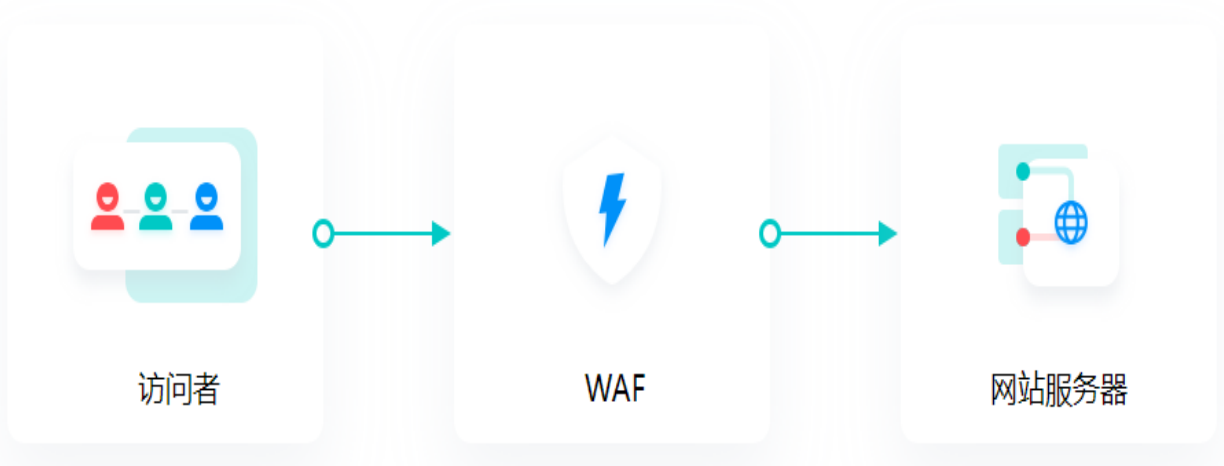
选题背景及内容

实现内容

为了更好的让部分中小企业和个人站点免受外部黑客攻击，因此我希望实现一个web应用防火墙（塔菲网络服务防御系统）

该系统主要功能是在访问者和网站服务器之间充当中间人，将访问者将流量先发送给WAF，再由WAF进行判断无恶意后再发送给网站服务器，从而实现对恶意流量的拦截，如图





PART
TWO

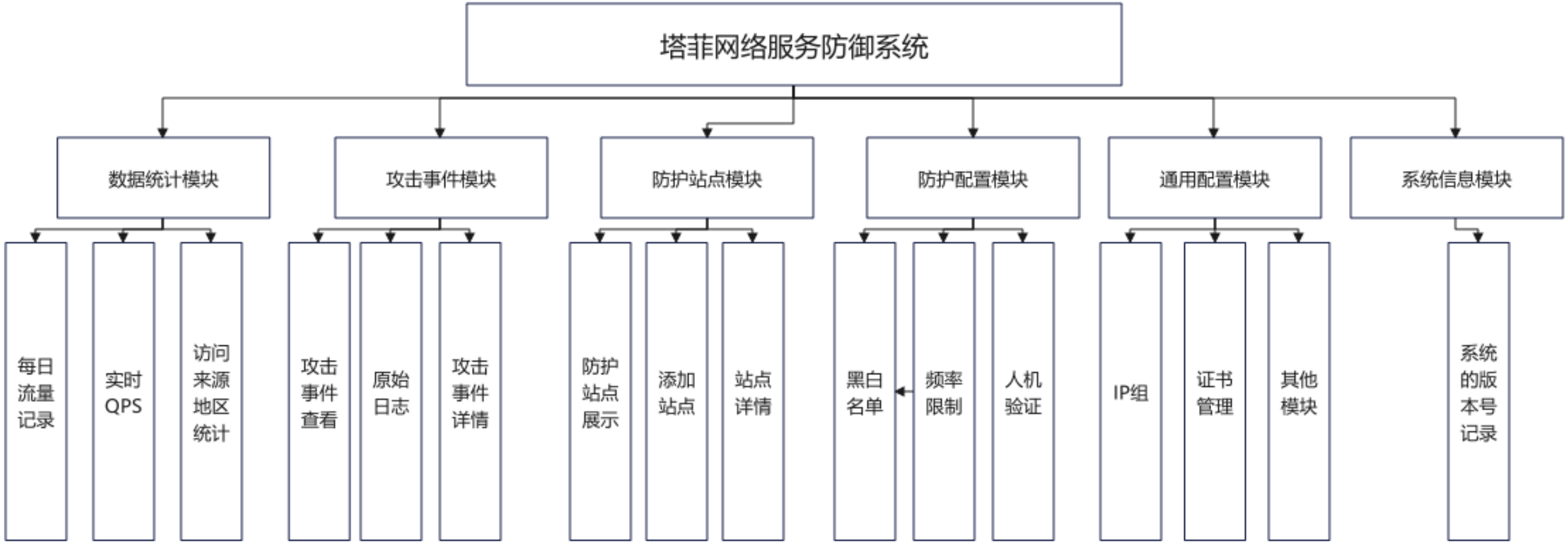
02

详细功能

详细功能

功能结构图

塔菲网络服务防御系统具体实现分为Web控制端和检测引擎两大部分，Web控制端功能界面如下：

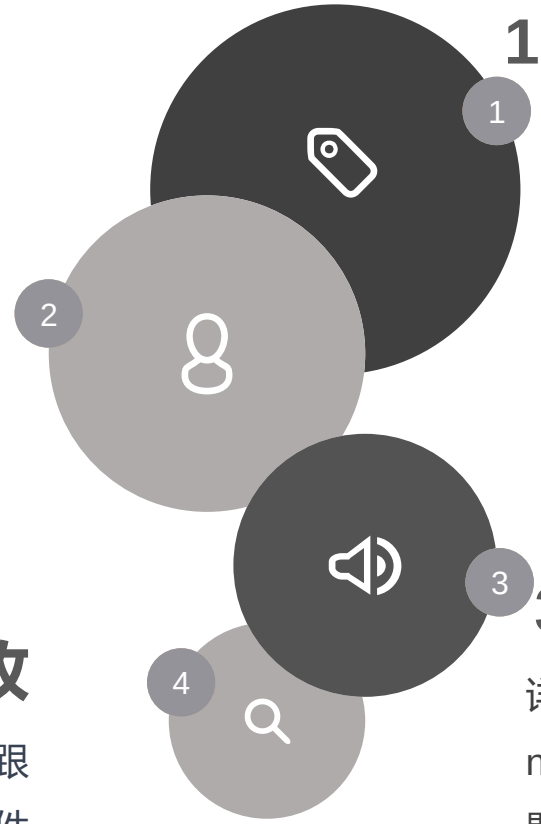


PART
THREE

03

技术栈及实现原理

实现原理



1.配置Nginx

模块加载：在nginx中配置加载检测引擎

监听端口：配置监听端口为web端口（例如80，443等）

转发规则： WAF设计为反向代理，确保所有请求都被转发到WAF进行处理，然后再转发到实际的应用服务器。

2.修改网站DNS记录

例如我想对x站进行防御，那么我就修改x站的a记录指向为nginx所在服务器的ipv4地址，或者修改cname记录为nginx所在服务器的域名地址

3.部署测试

详细经过：用户访问x站的80端口由于cname记录解析到nginx站的8080端口；Nginx站通过检测引擎判断请求包无问题放行，流量发送至x站的80端口；x站可以通过本地80端口判断请求包ip地址来源是否为nginx站若是则为转发后流量可直接域名解析到ip接收，若不是则cname转移至nginx站

4.配置修改

通过web控制端修改检测规则，监控系统来跟踪WAF的性能和安全事件

技术栈详细划分

管理容器

web控制端，负责WAF的配置管理、策略更新、用户界面后台行为等。

前端： React或Vue.js框架

后端： nodejs + Express框架

优势：统一前后端语言；语法简洁，开发效率高；nodejs框架安全性较高，组件漏洞少

检测容器

采用规则匹配型威胁检测和智能语义分析相结合的方式共同防御。

开发语言：Go

优势：高性能，直接编译成机器代码而不是中间代码或解释执行，这意味着Go编写的程序运行速度快；

日志容器

负责记录所有请求和攻击检测的日志，为后续的审计和分析提供数据

工具：使用Elasticsearch堆栈进行日志管理

网关

所有请求都会先经过网关再路由到相应的服务

类型：nginx

优势： Nginx提供了强大的反向代理功能和多种负载均衡策略

关系型数据库

存储攻击日志、保护站点、黑白名单配置的数据库

数据库类型：Mysql

优势：开源，低成本

缓存数据库

提供高速的数据读取和写入，改善性能和响应速度

数据库类型：redis

优势：支持主从复制，可以进行故障转移和读取负载均衡；将内存中的数据保存到磁盘中，即使在系统故障后也能恢复数据

PART
FOUR

04

可能遇到的问题和解决方案

可能遇到的问题和解决方案

1

性能与安全的平衡

问题：WAF需要实时分析和处理所有进入的HTTP/HTTPS请求，如果处理不够快，会增加网页加载时间

解决：采用负载均衡；采用非阻塞I/O和异步数据处理来减少延迟

2

准确性和误报

问题：用户输入的可能是正常内容导致误报，例如SQL注入拦截规则select. … from …，用户输入英文you should select good ideas from this lesson会被规则拦截

解决：采用智能语义分析技术，通过SQL引擎，SQL语法等判断

3

规则和算法的更新

问题：随着时间推移，可能发现新的规则绕过方式，例如文件上传漏洞的分块传输等

解决：完善特征库和规则集；允许用户自定义拦截规则；

4

兼容性和集成问题

问题：确保WAF在各种服务器环境和应用中运行，包括云环境、本地部署 、docker容器化部署

解决：在多种环境和配置中进行广泛测试

可能遇到的问题和解决方案

用户和配置管理

问题：用户是小白，配置和管理WAF应该简单直观，否则可能导致配置错误，影响效果

解决：用户友好的界面，提供图形界面，简化配置过程

法律和合规性问题

问题： WAF处理的数据可能涉及敏感信息

解决：加密敏感数据，确保传输和存储的安全，即支持自定义https证书

维护和支持

问题：若所采用的技术栈or框架爆出漏洞，例如CVE-2017-14849

解决：定期修复漏洞，更新版本

感谢您的观看

感谢您的观看！并提出宝贵意见

导师：王波　　答辩人：孙雷(20级软件工程2班)