附件：

**南山区医疗集团总部**

**web应用防火墙项目需求**

# 项目背景

随着互联网和移动互联网技术的快速发展，网站和各类Web应用近年呈现爆发式的增长，在电子政务、电子商务、组织流程、协作办公等领域得到广泛的应用，但与此同时，信息化的快速发展也带来诸多网络安全威胁等问题。

Web作为我单位面向广大公众/员工窗口，操作简易，易成为黑客首选目标；同时，由于网络便利性，攻击者可以轻易获取web攻击工具，不需要有深厚代码基础就能发起攻击。国家互联网应急中心（CNCERT）统计2021年上半年数据表明，我国全年恶意篡改的网站数量约为 3.4万个，植入后门的网站数量为 1.4万个。

目前已知的应用层攻击方法很多，攻击者通过应用层协议进入组织内部，如Web、Web邮件、聊天工具和P2P等攻击企业网络。利用攻击软件，攻击者不需要对网络协议的深厚理解基础，即可完成诸如更换Web网站主页、盗取管理员密码、破坏整个网站数据等等攻击。而这些攻击过程中产生的网络层数据，和正常数据没有什么区别。常见的威胁如下：

|  |  |
| --- | --- |
| 威胁名称 | 威胁描述 |
| 非授权访问 | 非授权用户可能试图访问和使用非授权端口、应用类型以及资源 |
| Web应用攻击 | 恶意用户可能通过构造特殊的HTTP/HTTPS请求，对产品保护的Web应用实施SQL注入、XSS等Web攻击 |
| 暴力认证 | 恶意用户可能通过反复猜测鉴别数据的方法，从而获取管理员权限 |
| 漏洞攻击 | 恶意用户可能利用产品本身或其所保护资产所存在的脆弱性，而对其发起远程攻击 |
| 敏感信息泄漏 | 用户的敏感信息（如银行卡账号，身份证号，手机号码等）或者服务器关键文件（如数据库信息文件，服务器配置文件等）遭到有意或者无意的泄漏 |
| 信息篡改 | 恶意用户篡改服务器文件，使得服务器信息以非正常方式呈现 |

我单位调研发现，大部分组织单位将大量的投资花费在网络和服务器的安全上，在网络中会部署防火墙、IPS、防病毒等安全产品，但是这类产品对于Http和Https的Web应用层攻击往往无法检测，没有从真正意义上保证 Web 业务本身的安全，才给黑客可乘之机，导致Web应用成为黑客的主要攻击目标。

# 项目周期

项目建设周期为60天。

# 项目需求

## 运维管理

南山区医疗集团总部拟搭建Web应用防火墙系统（下文简称：WAF），对其管理的Web应用系统实现Web应用安全防护。针对南山区医疗集团总部的网络拓扑结构和管理模式特点，Web应用防火墙系统应当满足以下方面需求：

1. 具备快速上线能力，对正常业务开展无明显影响；

2. 提供安全和人性化的管理交互界面，操作简单便捷；

3. 具备数据对接能力，便于同其他安全运维管理平台或设备实现联动；

4. 提供灵活的策略管理控制；

5. 提供人性化的统计报表与防护报告。

## 防护能力

WAF作为重要的Web应用层防护设备，应具备基于Http/Https协议的攻击检测和拦截能力，具体需求如下：

1. 具备较强的协议解码能力，防止攻击者利用多层编码进行绕过；

2. 支持识别OWASP TOP10安全威胁攻击；

3. 支持自定义Http协议防护规则，可灵活设定防护策略；

4. 具备一定0day攻击防御能力；

5. 支持可编程扩展插件，满足复杂业务模式下的业务安全防护需求。

## 部署模式

南山区医疗集团总部信息中心已规划建设虚拟化云环境，通过评估业务模式和网络架构，计划采购一套WAF平台软件，采用集群化反向代理部署模式。

## 处理性能

1. 单检测节点http每秒处理请求数不低于40000QPS。

2. 单检测节点https每秒处理请求数不低于4000QPS。

3. 数据延迟要求小于5ms。

## 高可用性

1. 软件应支持多模块冗余多活模式，当单个软件模块异常时，不影响系统正常运行；

3. 软件应支持在线扩容功能，可通过新增检测模块实现性能横向扩容。

# 技术分析

国内Web应用防火墙技术起步较晚，随着 Web安全问题日益严重，新兴安全厂商及诸多传统厂商也开始从事Web应用防火墙研究，并经历了如下阶段：

传统安全厂商研制出基于IPS架构的Web防火墙，本质上是增强IPS的Web安全模块功能，缺少细粒度的HTTP协议解析能力，缺乏特征匹配的能力，在实践中，用户发现达不到预期效果。

随后，国外安全厂商Imperva等推出以代理技术为基础的Web应用防火墙，防护能力强于基于IPS架构的防火墙，安全策略灵活，因此国内安全厂商也逐步转型，推向市场后得到了快速的发展，同时取缔了原先WAF，成为主流。

但是目前以代理作为基础的WAF仍存在业务冲突问题，其对安全特征库过度依赖，使得访问整体性能下降明显，安全规则库的维护也增加了运维人员的时间成本；同时，Web 攻击多样化、综合化，基于规则的 Web 应用防火墙很难识别 0day 攻击或者变种攻击。虽然安全厂商推出了自动学习网站业务建模，更有针对性、误判率也有降低，但是在 Web 业务复杂度极高的今天，并不能将安全保护覆盖到所有的业务线。

在安全情报快速传播、安全风险不断升级的信息时代，传统 WAF 产品面临巨大的安全防护挑战:

第一，传统 WAF 产品依赖规则来进行 Web 攻击防御:规则维护麻烦，且容易出错；误报率和漏报率都很高；难以跟踪未知漏洞。

第二，传统 WAF 产品主要以单台设备形式部署:难以处理大数据大流量；单点失效风险；管理麻烦。

第三，传统 WAF 产品无法形成安全的正向循环:阻挡攻击永远只是临时方案，修复漏洞才是最安全的途径；报表暂时无法带来实质的用处，有效的信息与风险分析才能带来决策支持。

根据上述调研结果，Web安全防护呈现出的新问题和新趋势，需要一种安全防护适应能力强、具有安全风险分析能力、能够进行系统水平扩展的新型 Web 应用安全防护系统，帮助应用管理人员全面提升Web安全防护水平。新一代WAF应基于以下几个特征或满足以下几个特点：

第一，采用基于语义算法的引擎，降低维护规则库的难度及精力损耗。采用非规则引擎，使用算法模型可以最大限度增强检测精准性(低误报、低漏报)，如检测SQL注入攻击时使用词法分析与语法分析技术、检测跨站脚本攻击时使用分层检测模型等，以最大的可能减少规则使用，无需维护，方便易用；同时也避免了规则叠加太多导致速度变慢的问题。

第二，具备优良的水平扩展架构。我单位业务部署在政务云上，流量峰值不稳定，需要WAF支持大流量大数据应用场景，必要时可考虑集群，无单点失效问题；同时，该集群可以将检测能力水平扩展，实现安全资源和云上资源一样，弹性伸缩。

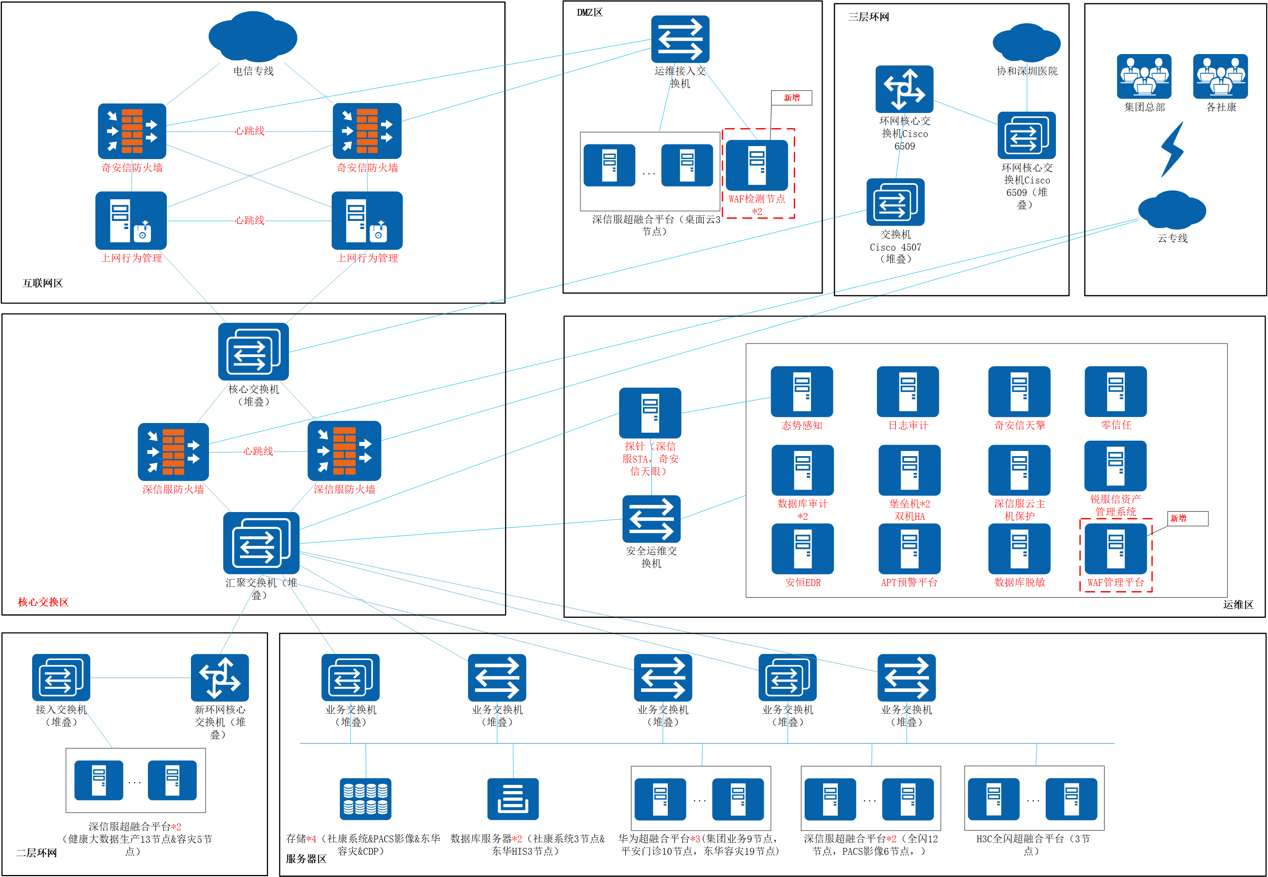
第三，构建安全正向循环，界面务必清晰展示攻击相关信息，能够快速定位恶意IP及攻击手法完成策略调整，同时具备日志payload以供溯源分析；将主动防御与被动信息处理相结合，形成拦截或报警，再到修复漏洞的正向循环。

# 建设内容

本次Web业务系统安全建设主要目的利用WAF专业的应用层安全防护技术，结合业务系统实际环境，解决针对WEB系统的入侵、漏洞、破坏等安全问题，以及被攻击绕过后产生的网页篡改、黑链、敏感信息泄露等问题，实现Web业务系统的全生命周期的安全防护。

# 方案设计

## 部署拓扑



## 系统功能实现

### OWASP十大web攻击防护

提供OWASP定义的十大安全威胁的攻击防护能力，有效防止常见的web攻击。（如，SQL注入、XSS跨站脚本、CSRF跨站请求伪造）从而保护网站免受网站篡改、网页挂马、隐私侵犯、身份窃取、经济损失、名誉损失等问题。



### 全开放的功能接口

具备全功能开放接口（Open API），所有页面功能均可通过API实现调用，可通过SoC或SIEM平台调取WAF检测日志、下发安全策略等，构建多平台、多设备的安全联动，提高安全和运维管理效率。应提供基于REST-ful的标准API接口，可快速融入现有安全运维体系。

### APi安全

除了针对HTTP/HTTPS的Web应用服务站点的防护外，也应支持针对API的防护，通过防护引擎对API流量进行安全检测，阻断攻击行为，有效的为微服务、小程序等提供安全防护。

### 可视化风险展示

产品应将检测到的业务系统的安全风险以图形化报表实时分类展示出来，如入侵风险、实时漏洞风险、数据风险和黑链风险等，并给出每一类安全风险的详细信息说明，让用户快速掌握现网安全状况。

### 弹性扩展适配新型应用场景

近年来，新基建带来的流量在逐渐增大，但是传统WAF上云时仅能安装在一个个单独的虚拟机中，导致集中管理、弹性伸缩等优秀特性很难发挥出来，新建设的WAF需要支持实现WAF集群统一管理、检测节点支持弹性扩展，在极低资源消耗的基础上实现高可用、高效率，且能够满足快速上线、灵活增减策略等易用性需求，适配新基建时期云时代大流量、智能计算的应用场景。

# 效益分析

本项目可以帮助我单位在信息化建设过程中，实现现有业务系统的整体全面的安全防护的目的，并带来以下几个效益 ：

## 有效提高Web安全防护能力

WAF对现有业务系统进行安全加固，有效抵御长期对用户Web业务影响最严重的安全攻击威胁，并防止各种安全威胁在系统内部扩散，确保用户关键应用正常稳定运行。通过创新性的威胁检测方法摆脱传统规则型的短板，通过内置各类编程语言编译系统，对攻击Payload进行语义分析，有效降低误报率和漏报率；在面对突发 0day漏洞威胁时，同样具备识别和防御能力。

## 满足合规性要求

Web应用防火墙为用户业务系统提供专业性的应用层安全防护，帮助用户满足等保测评、《网络安全法》、公安部82号令等行业法规的要求；能够满足安全可控的要求，保证自身从底层硬件到上层应用的安全自主；支持双协议栈技术，同时支持IPv4与IPv6网络协议， 能够满足IPv4向IPv6过渡阶段的网络部署需求。

## 简化日常安全运营工作

WAF应提供软件形态的交付方式，支持反向代理集群、嵌入式反向代理集群等多种软件部署模式，适合各类虚拟化平台部署环境。产品界面友好，无需维护庞杂的规则库，即可实现站点防护策略配置；具备良好的站点资产管理视角，我单位可按照站点灵活选取防护策略。对内，可以与蜜罐、态势感知平台等产品联动。

# 建设清单

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **序号** | **名称** | **数量** | **单位** | **性能要求** |
| 1 | web应用防火墙 | 1 | 套 | 1.单检测节点http每秒处理请求数不低于40000QPS。  2.单检测节点https每秒处理请求数不低于4000QPS。  3.数据延迟要求小于5ms。  4.Web攻击防护  5.提供全开放功能接口  6.提供api微服务防护  7.提供可视化风险展示大屏  8.支持软件集群部署，支持横向扩展检测节点 |