**中国医学科学院肿瘤医院**

**医保与APP防火墙技术需求**

**信息中心/计算机室**

**2021年9月**

目录

[第一部分：项目需求 3](#_Toc83741716)

[1.1. 项目背景 3](#_Toc83741717)

[1.2. 项目描述 3](#_Toc83741718)

[第二部分：技术需求 4](#_Toc83741719)

[2.1. 配置清单 4](#_Toc83741720)

[2.2. 产品技术要求 5](#_Toc83741721)

[第三部分：资质与服务要求 7](#_Toc83741722)

[3.1. 必要资质要求 7](#_Toc83741723)

[3.2. 非必要资质要求 7](#_Toc83741724)

[3.3. 服务要求 8](#_Toc83741725)

第一部分：项目需求

1. 项目背景

随着“互联网+”医疗和“健康中国2030”规划纲要的提出，国家层面越来越关注医院信息化建设的实用性，我院也及时顺应趋势，利用互联网的便利性，为患者提供了方便的挂号、支付、自助查询、在线问诊等互联网诊疗服务。这些功能主要通过“医科院肿瘤医院APP”来实现，该 APP是中国医学科学院肿瘤医院官方门户的手机应用,力求更好地解决看病难题,为广大病患提供更加方便快捷的就医通道。切实结合患者看病需求,集成预约挂号、手机缴费、智能分诊、科室医生、智能导诊等功能模块,通过互联网与移动终端的结合,最大程度的为患者简化就医流程,为实现高效、便捷、优质、低费用的医疗服务创造环境。

同时医保业务作为我院核心业务之一，稳定性可靠性要求非常高。近年来，医保系统多次发生勒索病毒内部扩散现象（通过 RDP暴力破解），对于医疗系统的网络安全和数据安全造成严重威胁。

因此医保业务系统边界和 APP 业务系统服务器边界亟需通过访问控制和应用层安全防护等相关技术手段进行安全能力建设，有效防范应用层攻击、区域内部跳板攻击等，提升相关业务的安全防护能力。

1. 项目描述

基于以上需求，本次计划采购 4 台下一代防火墙，其中 2 台部署在医保系统和内网核心交换机之间，2 台部署在 APP 业务服务器边界。通过部署下一代防火墙，开启ACL、入侵防御、防病毒模块，能够解决如下问题：

1）通过ACL进行边界访问控制，实现医保网络与医院网络的安全隔离，满足边界合规性要求。根据具体业务需求，在防火墙上配置精细的访问控制策略ACL，医保系统客户端和主机仅允许访问特定的目标，阻断非法访问和非法流量。

2）入侵防御，对抗来自第三方网络的攻击。检测来自专线的流量，实时、主动拦截黑客攻击、DDOS等恶意流量，防止操作系统和应用程序损坏或宕机。

3）开启网关防病毒模块，阻断恶意流量，防止主机中毒。依据病毒样本库，检测专线访问流量中是否隐藏病毒、木马、恶意插件等，避免内网服务器中毒。

4）僵尸主机检测，发现内网中毒主机。除了互联网下载病毒，带毒U盘、私人电脑等都有可能将病毒传播到医院内网，造成大量主机中毒；有的病毒（像勒索病毒）以破坏主机勒索用户为目的，而大多数病毒则是潜伏起来，被黑客利用进行数据窃取或对外发动DDOS攻击，下一代防火墙的僵尸主机检测功能可以检测内网已中毒主机，阻断通过专线的对外攻击流量，并实时告警。

第二部分：技术需求

1. 配置清单

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **项目** | **配置描述** | **数量** |
| 1 | 医保专线边界防火墙 | 设备网络层吞吐量≥20G，应用层吞吐量≥8G，FW吞吐量≥2.5G，并发连接数≥2200000，新建连接数（CPS）≥150000。标准机架式1U尺寸，内存大小≥8G，配置冗余电源，实配10/100/1000Base-T接口≥10个，千兆SFP接口≥4个，万兆SFP+接口≥2个。设备提供L2-L7层各类威胁的检测和防护，能够有效应对传统网络攻击和未知威胁攻击。实配防病毒模块、入侵防御模块和web 应用模块不少于3年。 | 2台 |
| 2 | APP应用边界防火墙 | 设备网络层吞吐量≥25G，应用层吞吐量≥9G，FW吞吐量≥3G，并发连接数≥2500000，新建连接数（CPS）≥200000。标准机架式2U尺寸，内存大小≥8G，配置冗余电源，实配10/100/1000Base-T接口≥6个，千兆SFP接口≥4个，万兆SFP+接口≥4个。设备提供L2-L7层各类威胁的检测和防护，能够有效应对传统网络攻击和未知威胁攻击。实配防病毒模块、入侵防御模块和web 应用模块不少于3年。 | 2台 |

注：所有实现项目功能需求所涉及的配件等，质保期内院方不再增加资金投入，均由投标方提供。

1. 产品技术要求

**医保专线边界防火墙（2 台）**

|  |  |
| --- | --- |
| **技术指标** | **指标要求** |
| 性能要求 | 设备网络层吞吐量≥20G，应用层吞吐量≥8G，FW吞吐量≥2.5G，并发连接数≥2200000，新建连接数（CPS）≥150000。标准机架式1U尺寸，内存大小≥8G，配置冗余电源，实配10/100/1000Base-T接口≥10个，千兆SFP接口≥4个，万兆SFP+接口≥2个。 |
| 网络特性 | 支持802.1Q VLAN Trunk、access接口，VLAN三层接口，子接口； 支持静态路由，ECMP等价路由；支持RIPv1/v2，OSPFv2/v3，BGP等动态路由协议；支持多播路由协议；支持多链路出站负载，支持基于源/目的IP、源/目的端口、协议、应用类型以及国家地域来进行选路的策略路由选路功能 |
| 基础功能 | 访问控制规则支持基于源／目的IP，源端口，源／目的区域，用户（组），应用/服务类型，时间组的细化控制方式；访问控制规则支持数据模拟匹配，输入源目的IP、端口、协议五元组信息，模拟策略匹配方式，给出最可能的匹配结果，方便排查故障，或环境部署前的调试；访问控制规则支持分组管理；支持根据国家/地区来进行地域访问控制； |
| 内容安全 | 内置病毒样本数量超过200万；支持URL过滤和文件过滤功能，URL过滤支持GET，POST请求过滤和HTTPS网站过滤，文件过滤支持文件上传和下载过滤；支持针对SMTP、POP3、IMAP邮件协议的内容检测，如邮件附件病毒检测、邮件内容恶意链接检测，邮件账号撞库攻击检测等，支持根据邮件附件类型进行文件过滤；支持采用无特征AI检测技术对恶意勒索病毒及挖矿病毒等热点病毒进行检测，给出基于AI技术的病毒检测报告。 |
| 入侵防护功能 | 设备具备独立的入侵防护漏洞规则特征库，特征总数在7000条以上； 支持对常见应用服务（HTTP、FTP、SSH、SMTP、IMAP、POP3、 RDP、Rlogin、SMB、Telne、Weblogic、VNC）和数据库软件（MySQL、Oracle、MSSQL）的口令暴力破解防护功能；可提供最新的威胁情报信息，能够对新爆发的流行高危漏洞进行预警和自动检测，发现问题后支持一键生成防护规则 |
| 安全可视化 | 支持资产的自动发现以及资产脆弱性和服务器开放端口的自动识别；支持自动生成安全风险报表，报表内容体现被保护对象的整体安全等级，发现漏洞情况以及遭受到攻击的漏洞统计，具备有效攻击行为次数统计和攻击举证；支持以攻击链方式来匹配和展示资产遭受到的攻击行为； |
| 系统配置管理 | 支持以安全策略模板方式快速部署安全策略，安全策略模板支持默认模板和自定义模板等多种格式；支持管理员权限分级，支持安全管理员、审计员、系统管理员三种权限；支持修改TCP，UPD和ICMP协议的连接超时时间；支持邮件、短信和微信告警； |

**APP应用边界防火墙（2 台）**

|  |  |
| --- | --- |
| **技术指标** | **指标要求** |
| 规格参数 | 设备网络层吞吐量≥25G，应用层吞吐量≥9G，FW吞吐量≥3G，并发连接数≥2500000，新建连接数（CPS）≥200000。标准机架式2U尺寸，内存大小≥8G，配置冗余电源，实配10/100/1000Base-T接口≥6个，千兆SFP接口≥4个，万兆SFP+接口≥4个。 |
| 产品形态 | 产品为专业的下一代防火墙产品。 |
| 部署方式 | 支持透明、路由、混合、旁路四种工作模式； |
| 网络适应性 | 支持静态路由，动态路由（OSPF、RIP、BGP等），ECMP等价路由，组播路由等； |
| 支持多链路负载均衡，可基于IP、协议、端口、应用类型及国家地域来进行智能选路。 |
| 网络访问控制 | 支持连接会话展示，可针对具体的IP地址进行会话详情查询，支持封锁异常会话信息，并支持设置监听具体IP的会话记录； |
| 访问控制规则支持基于源／目的IP，源端口，源／目的区域，用户（组），应用/服务类型，时间组的细化控制方式，支持长连接功能并可以配置连接时长；  |
| 防病毒功能 | 支持URL过滤，支持GET，POST请求过滤和HTTPS网站过滤； |
| 支持针对SMTP、POP3、IMAP邮件协议的内容检测，如邮件附件病毒检测、邮件内容恶意链接检测，邮件账号撞库攻击检测等，并给出恶意邮件的提示，支持根据邮件附件类型进行文件过滤；  |
| 支持采用无特征AI检测技术对恶意勒索病毒及挖矿病毒等热点病毒进行检测，给出基于AI技术的病毒检测报告。  |
| 产品支持勒索病毒检测与防御功能，为保障勒索病毒的防御效果，须具备权威机构关于“勒索软件通信防护”功能项的产品检测报告。 |
| 安全防护功能 | 设备具备独立的IPS漏洞规则特征库，具备7000种以上攻击特征库规则；  |
| 支持对常见应用服务（HTTP、FTP、SSH、SMTP、IMAP、POP3、 RDP、Rlogin、SMB、Telnet、Weblogic、VNC）和数据库软件（MySQL、Oracle、MSSQL）的口令暴力破解防护功能； |
| 可提供最新的威胁情报信息，能够对新爆发的流行高危漏洞进行预警和自动检测，发现问题后支持一键生成防护规则。 |
| 产品支持CC攻击防护功能，为保障勒CC攻击的检测效果，须具备权威机构关于“CC攻击防护”功能项的产品检测报告。 |
| 僵尸主机检测 | 设备具备独立的热门威胁库，防护类型包括木马远控、恶意脚本、勒索病毒、僵尸网络、挖矿病毒等，特征总数在60万条以上；  |
| 支持木马远控类、恶意链接类、移动安全类、异常流量类僵尸网络行为的检测。  |
| 支持对终端已被种植了远控木马或者病毒等恶意软件进行检测，并且能够对检测到的恶意软件行为进行深入的分析，展示和外部命令控制服务器的交互行为和其他可疑行为。 |
| 对于未知威胁具备同云端安全分析引擎进行联动的能力，上报可疑行为并在云端进行沙盒检测，并下发威胁行为分析报告；  |
| 支持通过云端的大数据分析平台，发现和展示整个僵尸网络的构成和分布，定位僵尸网络控制服务器的地址；  |
| 安全可视化 | 支持资产的自动发现以及资产脆弱性和服务器开放端口的自动识别； |
| 支持安全运营中心功能，可以对全网所有的服务器和主机的威胁进行全面评估，管理员通过一键便可完成对服务器和主机的资产更新识别、脆弱性评估、策略动作的合理化监测、当前服务器和用户的保护状态、当前的服务器和主机的风险状态及需要管理员待办的紧急事项等，可以自动化直观的展示最终的风险。 |
| 支持自动生成安全风险报表，报表内容体现被保护对象的整体安全等级，发现漏洞情况以及遭受到攻击的漏洞统计，具备有效攻击行为次数统计和攻击举证； |

注: 1、投标人须如实响应技术指标要求。 2、产品供货后，采购人将对中标产品进行性能测试和功能验证，与投标承诺不符将做为无效投标处理，由此引发的所有损失由该投标人承担。

第三部分：资质与服务要求

1. 必要资质要求

1、要求产品具备公安颁发的计算机信息系统安全专用产品销售许可证，提供证书复印件并加盖公章。

2、要求产品具备国家版权局颁发的软件著作权登记证书，提供证书复印件并加盖公章。

3、为保障技术标准先进性，要求所投产品的生产厂商参与制定《信息安全技术第二代防火墙安全技术要求》，提供证书复印件加盖公章。

4、产品应具备ISCCC中国国家信息安全产品认证证书，提供证书复印件并加盖公章。

1. 非必要资质要求

1、为保障安全服务能力，要求产品生产厂商为网络安全应急服务支撑单位（国家级），提供证书复印件并加盖公章。

2、为保障安全开发能力，要求所投产品的生产厂商具备中国网络安全审查技术与认证中心（CCRC）颁发的《软件安全开发服务》资质证书，提供证书复印件并加盖公章。

3、为保障技术可靠性，要求产品生产厂商具备能力成熟度模型集成/软件能力成熟度模型 5 级认证证书(CMMI L5)，提供证书复印件并加盖公章

1. 服务要求

本项目须提供生产原厂商针对本项目的3年售后服务承诺函。