## 信息安全软件需求

**一、等保测评**

## 项目背景分析

成都市公共卫生临床医疗中心依据《中华人民共和国网络安全法》的相关要求，对本单位的信息系统进行网络安全等级保护测评工作。

本次信息安全等级保护测评涵盖安全技术内容包括：安全技术测评：包括安全物理环境、安全通信网络、安全区域边界、安全计算环境和安全管理中心等五个方面的安全测评。安全管理测评：包括安全管理制度、安全管理机构、安全管理人员、安全建设管理和安全运维管理等五个方面的安全测评。依据相关的测评准则，结合系统的构成特点，确定具体的测评对象，制定测评方案，通过访谈、检查、测评和系统分析等方式判断其安全技术和安全管理的各方面是否达到了相应等级的国家信息系统等级保护要求，找出信息系统中存在的安全隐患，对安全性进行整体评估，制定相关的信息安全整体安全策略和中长期的安全规划，以便对被测系统进行安全方面的调整和改进，确保其安全防护水平达到信息系统安全等级保护相应能力的要求。

## 项目需求

|  |  |  |
| --- | --- | --- |
| **系统名称** | **安全保护等级** | **测评地点** |
| HIS | 三级 | 医院 |
| LIS | 三级 | 医院 |
| PACS | 三级 | 医院 |
| EMR | 三级 | 医院 |
| 微信 | 三级 | 医院 |
| 网站 | 三级 | 医院 |

## 项目实施标准

### 测评依据

 《中华人民共和国网络安全法》

 《信息安全等级保护管理办法》（公通字[2007]43号）

 GB/T 22239-2019信息安全技术 网络安全等级保护基本要求

 GB/T 22240-2020信息安全技术 网络安全等级保护定级指南

 GB/T 25070-2019信息安全技术 网络安全等级保护安全设计技术要求

 GB/T 28449-2018 信息安全技术 网络安全等级保护测评过程指南

 GB/T 28448-2019信息安全技术 网络安全等级保护测评要求

 GB/T 18336.1-2008信息技术 安全技术 信息技术安全性评估准则

 GBT 25070-2019信息安全技术 网络安全等级保护安全设计技术要求

### 测评原则

**保密性要求**

我公司与采购人签订保密协议，对测评的过程数据和结果数据严格保密，未经采购人授权不得泄露相关信息给任何单位和个人，不得利用此数据侵害采购人的权益，否则采购人有权追究我公司的责任。

**标准性要求**

我公司的测评方法及评估方案的设计与实施都是依据国家的相关标准进行。

**规范性要求**

我公司在项目实施过程中按照项目管理规范对工作中产生的过程文档进行管理，便于项目跟踪和控制。

**可控性要求**

我公司根据项目实际情况提供项目安排计划保证采购人对测评工作的可控性。

**整体性要求**

测评及评估的范围和内容满足等级保护2.0的相关基本要求。

**系统运行要求**

技术测评及评估工作不对现有运行系统造成影响。若评估可能会影响在线系统运行的应提供系统保障方案经采购人同意后进行。

1. **网络管理平台**

随着网络规模的扩大，接入主机的增多和复杂网络应用的开展．网络管理的重要性日益显现，需通过结合[软件](https://baike.baidu.com/item/%E8%BD%AF%E4%BB%B6/12053" \t "https://baike.baidu.com/item/%E7%BD%91%E7%BB%9C%E7%AE%A1%E7%90%86%E7%B3%BB%E7%BB%9F/_blank)和[硬件](https://baike.baidu.com/item/%E7%A1%AC%E4%BB%B6/479446" \t "https://baike.baidu.com/item/%E7%BD%91%E7%BB%9C%E7%AE%A1%E7%90%86%E7%B3%BB%E7%BB%9F/_blank)用来对[网络状态](https://baike.baidu.com/item/%E7%BD%91%E7%BB%9C%E7%8A%B6%E6%80%81" \t "https://baike.baidu.com/item/%E7%BD%91%E7%BB%9C%E7%AE%A1%E7%90%86%E7%B3%BB%E7%BB%9F/_blank)进行调整的系统，以保障网络系统能够正常、高效运行，使网络系统中的资源得到更好的利用。具体要求如下：

**设备管理**

　　用户可以方便的管理设备及其配置参数。支持在拓扑图的基础上，进一步展示设备细节，包括设备的物理组件，服务器上的服务（Web服务器、中间件应用服务、数据库服务器、邮件服务器）或者用户定义的其他监控对象。

**故障管理**

　　采用多种告警机制，自定义配置告警阀值，支持快速标示已经执行操作的告警，迅速定位告警设备。全面采集设备资源、应用、服务等告警信息。可将告警信息数据按照时间、资源、性能类型等多种维度以图表等形式展现。通过对告警机制以及阀值的设置，第一时间获取准确的告警信息，快速定位告警设备。

**配置管理**

　　支持同时对每多台设备进行配置/备份和软件升级，以减少管理员的工作量，提高系统的可用性。支持单个和批量设备的配置文件升级、备份和恢复功能。网管软件自带ftp服务器。

配置管理：下发配置文件到一台/多台设备；定期备份设备配置文件。

设备软件管理：自动/手工升级软件为预设版本；生成手动/自动升级结构报告。

设备参数管理：可配置VLAN、QOS、ACL、网络限速以及优先级等参数。

**性能管理**

全面采集设备资源、应用、服务等性能信息。可将性能信息数据按照时间、资源、性能类型等多种维度以图表等形式展现。

**安全管理**

　　采用多级网络/区域的组织结构，且可以对不同的用户分配管理不同的网络/区域。用户登陆后只能看到自己权限下的网络和设备。黑白名单功能用来检测用户所关心的设备（通过IP或MAC来识别）是否在网络中出现及出现时间，一提醒用户是否进行下一步的操作。

**简单网络管理协议SNMP**

　　简单网络管理协议SNMP是设计为工作在TCP／IP协议上的网络协议，基于TCP／IP协议工作，对网络中支持SNMP协议的设备进行管理。

　　SNMP协议为网络管理员提供了一个统一的界面。不论网络设备的型号、生 产厂商如何，只要设备支持SNMP协议，管理员都可以通过统一的操作进行网 络管理。这样就可把管理员的精力集中于网络的组织与管理而不是各网络设备之间的差别。

**网管软件的实现**

   网络管理应用非常广泛，具有以下几个优点：

1、设计简单。使用SNMP管理网络设备，既不需要复杂的实现过程，也不会占用太多的网络资源，非常便于使用。

2、应用广泛。大多数网络设备厂商在设计和生产网桥、路由器等设备时都加入了对SNMP的支持。

3、良好的可扩展性。SNMP协议较为简单，对协议的升级货扩展方便，能够满足今后网络发展的需求。

网管平台兼容主流/国产系统及数据库，提供B/S客户端界面，兼容PC以及移动设备。已实现包括设备拓扑、故障管理、性能管理、配置管理以及安全管理等在内的超过1000种基础网管功能。采用SNMP协议，支持管理管理网络设备、计算机、服务器、智能设备、物联网、工业设备等所有支持SNMP协议的设备，适用于医疗、国防、电信、政府、金融、交通、能源、企业、工业、制造等多种领域。

　　网管平台采用J2SE、XML、Web Service、Web、HTML5、JavaScript、Struts、Spring、Hibernate、SNMP、HTTP、JDBC、Swing、RMI、O-M Mapping、O-R Mapping、Muti-Thread等成熟技术。由表示层、业务层、数据层和设备中间层多层次架构模式组成，提供corba和webservice接口。在框架上采用设备中间层屏蔽不同厂商设备管理协议的差异，实现支持管理不同类型的被管设备。

**网管的功能实现**

**自动发现：**在自动发现的过程中可搜索到网络设备，并识别设备类型和厂商型号，生成设备的面板图或搜索设备资源，如：板卡、端口、CPU、内存、磁盘等，并发现设备之间的链路关系。

**拓扑管理：**以具象化拓扑图方式展示网络设备及其连接关系，用户可编辑。通过拓扑图可以对设备、设备资源、连接进行管理。

**设备管理：**通过拓扑视图中，用户可以方便的管理设备及其配置参数。

**设备资源管理：**支持在拓扑图的基础上，进一步展示设备细节，包括设备的物理组件，服务器上的服务（Web服务器、中间件应用服务、数据库服务器、邮件服务器）或者用户定义的其他监控对象。

**连接管理：**用户可以通过拓扑视图编辑连接，选择连接实时显示的性能数据项。

**故障管理：**可以收集多种故障信息，并及时的展现出来，通过设备、资源、连接可以查看到故障信息，也可以通过统一的故障管理界面管理故障。

**事件管理：**可以设备/服务器主动发送的消息，集中处理后，及时的通知用户，并可以通过集中的管理界面进行管理。

**安全管理：**支持多级网络/区域的组织结构，且可以对不同的用户分配管理不同的网络/区域。用户登陆后只能看到自己权限下的网络和设备。黑白名单功能用来检测用户所关心的设备（通过IP或MAC来识别）是否在网络中出现及出现时间，一提醒用户是否进行下一步的操作。

**配置管理：**支持同时对每多台设备进行配置/备份和软件升级，以减少管理员的工作量，提高系统的可用性。

**网络工具：**集成了常用的网络管理工具，支持用户的配置参数。

**性能管理：**全面采集或接收设备资源的多种新能数据，通过曲线图、柱状图或表格等形象化的展示出来，按天、星期、月 查看性能指标变化。

**统计报表：**支持多项数据的统计功能，让用户对网络有一个全面直观的了解放。支持将软件中的统计图表导出或打印，以便备份或对比查看。

**技术参数如下：**

1. ▲要求资源拓扑、告警、性能等功能模块支持多服务器分布式虚拟化部署，可实现负载分担。
2. 用户分权管理：可以为不同的管理员设置不同的用户名、密码，并限制管理员的管理权限和管理范围，实现用户分权管理。
3. 多平台支持：支持Windows、Linux平台及MS SQL、Oracle、Cache数据库，支持B/S架构。
4. ▲支持自定义用户主页：管理员可以首页中通过拖拽，自定义需要在首页展示页面，提供软件页面截图，加盖原厂鲜章；
5. 自动发现拓扑：自动发现网络中的所有网络设备，并在拓扑中显示出来，支持拓扑图自定义修改，包括设备、链路等,提供软件页面截图，加盖原厂鲜章；。
6. 支持网络管理平台实现设备管理与流量分析联动，如通过点击拓扑某链路可查看该链路的关键应用流量分布、关键用户流量使用等,提供软件页面截图，加盖原厂鲜章；;
7. ▲支持设备面板的显示、定时刷新、面板缩放功能，通过面板管理，网络管理人员可以直观地看到设备、板卡、端口的工作状态。提供软件页面截图，加盖原厂鲜章；
8. ▲支持批量的设备配置备份和恢复。支持向导方式或者任务方式（周期性任务、一次性任务或立即任务）批量的备份、恢复完整的配置文件，也可以批量的下发配置片断。提供软件页面截图，加盖原厂鲜章；；
9. 提供设备运行配置和启动配置的基线化版本管理，将每个设备相关的配置文件划分为三种版本：基线、普通、草稿。便于管理员识别、管理。通过备份、恢复手段，以及备份历史、升级历史管理，使配置文件管理和软件升级管理具有了可回溯性，提供软件页面截图，加盖原厂鲜章；；
10. ▲接收Syslog，完成基本格式的解析，并入库,提供Syslog特征分析及策略注册能力，支持基于统计规则进行聚合生成告警（Trap），提供软件截图，加盖原厂鲜章;
11. ▲提供IOS、Android移动客户端查询特定设备功能，可浏览存在故障的设备信息及接口信息，对设备进行可达性测试（Ping，TraceRoute）等操作（提供软件使用界面截图，并加盖原厂鲜章）
12. VLAN拓扑功能以可视的方式对网络中的VLAN资源进行管理，查看拓扑视图中所有设备节点和链路是否允许某个特定VLAN通过。提供软件页面截图，加盖原厂鲜章；；
13. 为了方便设备管理，提供超长离线设备自动删除，可设置离线删除时间，提供软件页面截图，加盖原厂鲜章；
14. 提供天报表、周报表、月报表、季度报表、半年报表、年报表,提供软件页面截图，加盖原厂鲜章；;
15. ▲支持代理和免代理两种模式，可根据不同的场景选择不同的监控模式，也可同时使用。
16. ▲提供服务器Agent代理，可批量部署，无需服务器用户名和密码即可获取相关应用性能数据。支持断网容错，可保存24小时数据，网络恢复后数据自动上传到应用管理服务器。提供产品界面截图，加盖原厂鲜章；
17. ▲支持agent程序远程推送、远程安装、安装环境自检、远程升级、远程重启等，提供产品界面截图，加盖原厂鲜章；
18. 支持在非agentless方式下，采用telnet，ssh，WMI，IPMI，,JMX等协议采集监控应用数据；
19. ▲支持分布式部署，可部署到多台服务器上，实现负载分担。单套软件可管理应用节点数不小于1000个，须提供同等规模项目合同证明文件，加盖原厂鲜章；
20. 提供对常见操作系统的监控管理,包括Windows、AIX、IBM AS400 / iSeries、FreeBSD/OpenBSD、HP-UX/Tru64、Linux、Mac OS、Sun Solaris、中标麒麟等操作系统；
21. 提供对常见数据库服务器的监控管理,包括Cache 、MySQL、Oracle、MS SQL、DB2、informix、PostgreSQL、达梦、自定义SQL查询等；
22. ▲提供对常见应用服务器的监控管理，包括微软.NET、GlassFish、Jboss、OracleAS、SilverStream、Tomcat；
23. ▲提供对常见中间件服务器的监控管理，包括WebLogic Integration，支持Exchange2003、Exchange2007、SMTP、POP3型邮件服务器；
24. ▲提供对常见Web服务器和HTTP URL的监控管理，包括Apache、IIS、SOAP 服务、Rest 服务，支持URL/多个URL的监视和录制；
25. ▲提供对其他应用的监控管理，包括SAP CCMS、AD/LDAP、Ping、Telnet、SNMP、DNS、FTP/SFTP、文件服务、网络接口等；
26. ▲可通过IPMI协议监控X86服务器硬件信息，例如服务器风扇、电源状态，服务器机箱温度等。提供产品界面截图，加盖原厂鲜章；
27. ▲自定义应用类型监控：使用者可自行设计应用监控类型，灵活设计展示指标及页面布局。提供详细的应用开发指导文档，加盖原厂鲜章；
28. 报表管理：具备强大的报表功能，可以生成多种基于业务的分组报表，提供日报、周报、月报、年报等周期性报表，并自动发送到指定信箱。报表可以保存为各种格式，如PDF、Excel、CSV；还可以E-mail报表或打印报表；