**XXXXXXXXXX**

**信息安全等级保护服务项目**

**预**

**算**

**方**

**案**

**广东南方信息安全研究院**

**2017年8月**

目录

[1 概述 3](#_Toc490850811)

[1.1背景介绍 3](#_Toc490850812)

[1.2遵循依据 3](#_Toc490850813)

[1.3编制原则 4](#_Toc490850814)

[1.4项目目标 5](#_Toc490850815)

[1.5项目必要性 5](#_Toc490850816)

[2 安全需求分析 6](#_Toc490850817)

[2.1网络安全现状 6](#_Toc490850818)

[2.2初步风险分析 6](#_Toc490850819)

[2.3二级系统测评指标 7](#_Toc490850820)

[2.4需求分析 15](#_Toc490850821)

[3 方案总体规划 16](#_Toc490850822)

[3.1规划目标 16](#_Toc490850823)

[3.2整改产品规划 16](#_Toc490850824)

[3.2.1网络结构优化 16](#_Toc490850825)

[3.2.2边界安全防护 17](#_Toc490850826)

[3.2.3网络环境安全防护 22](#_Toc490850827)

[3.2.4主机安全防护 28](#_Toc490850828)

[3.2.5整改产品规划示意图 30](#_Toc490850829)

[3.3信息安全服务建议 30](#_Toc490850830)

[3.3.1定级备案协助 30](#_Toc490850831)

[3.3.2安全差距评估 31](#_Toc490850832)

[3.3.3安全整改设计 34](#_Toc490850833)

[3.3.4人工安全策略加固 35](#_Toc490850834)

[3.3.5管理制度建设与优化 36](#_Toc490850835)

[3.3.6等级保护验收测评 37](#_Toc490850836)

[3.3.7定期安全巡检 42](#_Toc490850837)

[3.3.8应急响应 43](#_Toc490850838)

[3.3.9网络安全培训 44](#_Toc490850839)

[3.3.10安全建设咨询 45](#_Toc490850840)

[4 项目整体清单预算 45](#_Toc490850841)

# 概述

## 背景介绍

自1994年国务院颁布《中华人民共和国信息系统安全保护条例》，要求信息系统分等级进行安全保护起，信息系统安全等级保护工作就已经成为我国信息安全领域的重中之重。随着近年来，各类信息泄露、网络诈骗、病毒攻击等安全事件日益频发，国家高度重视网络安全，于今年6月1日正式施行的《中华人民共和国网络安全法》第二十一条中，明确提出了“国家实行网络安全等级保护制度。网络运营者应当按照网络安全等级保护制度的要求，履行下列安全保护义务，保障网络免受干扰、破坏或者未经授权的访问，防止网络数据泄露或者被窃取、篡改….”。

因此开展及落实好信息安全等级保护工作是保障网络安全的基础，是提高单位信息安全保障水平的第一步，是防范各类安全事件的重要手段，也是做好国家信息安全、保障社会稳定的必要条件。

## 遵循依据

方案的编制遵循以下相关法律法规和标准：

**（一）法律法规：**

* 1. 《中华人民共和国网络安全法》；
  2. 《中华人民共和国计算机信息系统安全保护条例》（国务院147号令）；
  3. 《国家信息化领导小组关于加强信息安全保障工作的意见》（中办发[2003]27号）；
  4. 《关于印发<关于信息安全等级保护工作的实施意见>的通知》（公通字[2004]66号文）；
  5. 《关于印发<信息安全等级保护管理办法>的通知》（公通字[2007]43号文）；
  6. 《关于开展全国重要信息系统安全等级保护定级工作的通知》（公信安[2007]861号文）；
  7. 《广东省深化信息安全等级保护工作方案》(粤公通字[2010]45号)；
  8. 《国家网络与信息安全协调小组关于开展信息安全风险评估工作的意见》（国信办[2006]5号）。

**（二）技术标准：**

1. 《信息安全技术 信息系统安全等级保护基本要求》（GB/T 22239-2008）；
2. 《信息系统安全等级保护定级指南》（GB T 22240-2008）
3. 《信息安全技术 信息系统安全等级保护测评过程指南》；
4. 《信息安全技术 信息系统安全等级保护实施指南》；
5. 《信息安全技术 信息系统安全等级保护测评要求》；
6. 《信息安全技术 信息系统安全等级保护安全设计技术要求》（信安秘字[2009]059号）；
7. 《信息安全技术 网络基础安全技术要求》（GB/T20270-2006）；
8. 《信息安全技术 操作系统安全技术要求》（GB/T20272-2006）；
9. 《信息安全技术 数据库管理系统安全技术要求》（GB/T20273-2006）；
10. 《信息安全技术 服务器技术要求》（GB/T21028-2007）；
11. 《信息安全技术 终端计算机系统安全等级技术要求》（GA/T671-2006）；

除上述规范以外，还遵循国家现行的相关标准和规范要求。

## 编制原则

项目的方案设计满足以下原则：

**符合性原则**：符合国家信息安全等级保护制度及相关法律法规，指出防范的方针和保护的原则。

**标准性原则**：方案设计与建议依据国内、国际的相关标准进行。

**整体性原则**：方案中的安全体系设计的范围和内容应当整体全面，包括安全涉及的各个层面，避免由于遗漏造成未来的安全隐患。

**保密原则**：对方案中获得的数据和结果严格保密，未经授权不得泄露给任何单位和个人，不得利用此数据和结果进行任何侵害用户单位利益的行为。

## 项目目标

等级保护工作的目的是建立健全XXXXXXXXXX信息安全等级保护机制，对已有已建信息系统作安全状况测试，找出差距并进行安全整改与验收，使信息系统信息安全在技术和管理上达到等级保护的要求，进一步提升XXXXXXXXXX信息安全工作水平。本项目具体将达到如下目标：

1.完成XXXXXXXXXX信息系统安全等级保护定级备案工作，编制信息系统安全等级保护定级报告及备案资料，并取得国家信息安全等级保护主管部门出具的信息系统等级保护备案证；

2.完成XXXXXXXXXX信息系统安全差距评估，根据评估结果出具安全评估报告，提交全面、详细的安全整改建议；

3.根据安全整改建议结合等级保护二级标准完成安全整改工作；

4.根据安全整改结果，完成验收测评并提交符合国家信息安全等级保护主管部门要求的验收测评报告，通过国家信息安全等级保护主管部门的最终测评验收。

## 项目必要性

通过信息安全等级保护工作，主要实现以下3方面的重要意义：

1、满足国家政策法律要求。《网络安全法》中第八条明确规定了各部门在网络安全方面的职责分工，第二十一条规定了网络运营者应当按照网络安全等级保护制度，履行安全保护义务。第五十九条规定了对网络运营者和关键信息基础设施的运营者不履行网络安全保护义务需要承担的法律责任。同时《刑法修正案（九）》第二百八十六条之一规定了网络服务提供者不履行法律、行政法规规定的信息网络安全管理义务需要承担的刑事责任。

2、促进和提高单位信息安全保障水平。以等级保护为标准开展安全建设，可以从物理、网络、主机、应用和数据多个方面成体系保障单位的信息安全环境。

3、有利于国家安全、社会稳定。重点保障基础信息网络和关系国家安全、经济命脉、社会稳定等方面的重要信息系统的安全；有利于明确国家、法人和其他组织、公民的信息安全责任，加强信息安全管理。

# 安全需求分析

## 网络安全现状

XXXXXXXXXX信息系统网络拓扑如下：

## 初步风险分析

根据目前的网络拓扑环境结合《信息系统安全等级保护基本要求》、《网络安全法》中针对信息系统的相关安全防护规定，分析存在着如下安全问题与风险：

1. **可用性方面：**随着网络业务、信息流量等日益发展与增速的环境下，防火墙作为核心的数据转发与交换将不能满足业务对于处理速度、可靠性的需求，容易产生网络延迟、数据丢包等现象。且单点部署的产品很可能出现故障造成网络和业务中断的风险，将会影响整个网络业务的运行。
2. **网络环境安全方面：**信息系统没有完整的准入控制机制、安全审计机制、运维控制与审计措施。存在非授权用户连接入系统访问系统资源的风险，存在着出现安全问题无法追踪及溯源。
3. **终端安全方面：**缺少对终端的统一病毒防范，对终端的软硬件、移动介质、接入访问、安全补丁更新、病毒防范等状况进行统一监控。

## 系统测评指标

**等级保护二、三级测评指标（注：基本要求内加粗字体为等级保护三级所包含测评指标，未加粗字体为等级保护二级标准）。**

|  |  |  |  |
| --- | --- | --- | --- |
| **分类** | **子类** | **基本要求** | **测评项数** |
| 物理安全 | 物理位置的  选择 | 机房和办公场地应选择在具有防震、防风和防雨等能力的建筑内 | 2 |
| **机房场地应避免设在建筑物的高层或地下室，以及用水设备的下层或隔壁** |
| 物理访问  控制 | 机房出入口应安排专人值守，控制、鉴别和记录进入的人员 | 4 |
| 需进入机房的来访人员应经过申请和审批流程，并限制和监控其活动范围 |
| **应对机房划分区域进行管理，区域和区域之间设置物理隔离装置，在重要区域前设置交付或安装等过渡区域** |
| **重要区域应配置电子门禁系统，控制、鉴别和记录进入的人员** |
| 防盗窃与防破坏 | 应将主要设备放置在机房内 | 6 |
| 应将设备或主要部件进行固定，并设置明显的不易除去的标记 |
| 应将通信线缆铺设在隐蔽处，可铺设在地下或管道中 |
| 应对介质分类标识，存储在介质库或档案室中 |
| **应利用光、电等技术设置机房防盗报警系统** |
| **应对机房设置监控报警系统** |
| 防雷击 | 机房建筑应设置避雷装置 | 3 |
| **应设置防雷保安器，防止感应雷** |
| 机房应设置交流电源地线 |
| 防火 | **机房应设置火灾自动消防系统，能够自动检测火情、自动报警，并自动灭火** | 3 |
| **机房及相关的工作房间和辅助房应采用具有耐火等级的建筑材料** |
| **机房应采取区域隔离防火措施，将重要设备与其他设备隔离开** |
| 防水和防潮 | 水管安装，不得穿过机房屋顶和活动地板下 | 4 |
| 应采取措施防止雨水通过机房窗户、屋顶和墙壁渗透 |
| 应采取措施防止机房内水蒸气结露和地下积水的转移与渗透 |
| **应安装对水敏感的检测仪表或元件，对机房进行防水检测和报警** |
| 防静电 | **主要设备**应采用必要的接地防静电措施 | 2 |
| **机房应采用防静电地板** |
| 温湿度控制 | 机房应设置温、湿度自动调节设施，使机房温、湿度的变化在设备运行所允许的范围之内 | 1 |
| 电力供应 | 应在机房供电线路上配置稳压器和过电压防护设备 | 4 |
| 应提供短期的备用电力供应，至少满足**主要设备**在断电情况下的正常运行要求 |
| **应设置冗余或并行的电力电缆线路为计算机系统供电** |
| **应建立备用供电系统** |
| 电磁防护 | **应采用接地方式防止外界电磁干扰和设备寄生耦合干扰** | 3 |
| 电源线和通信线缆应隔离铺设，避免互相干扰 |
| **应对关键设备和磁介质实施电磁屏蔽** |
| 网络安全 | 结构安全 | 应保证**主要网络设备**的业务处理能力具备冗余空间，满足业务高峰期需要 | 7 |
| 应保证**网络各个部分的带宽**满足业务高峰期需要 |
| **应在业务终端与业务服务器之间进行路由控制建立安全的访问路径** |
| 应绘制与当前运行情况相符的网络拓扑结构图 |
| 应根据各部门的工作职能、重要性和所涉及信息的重要程度等因素，划分不同的子网或网段，并按照方便管理和控制的原则为各子网、网段分配地址段 |
| **应避免将重要网段部署在网络边界处且直接连接外部信息系统，重要网段与其他网段之间采取可靠的技术隔离手段** |
| **应按照对业务服务的重要次序来指定带宽分配优先级别，保证在网络发生拥堵的时候优先保护重要主机** |
| 访问控制 | 应在网络边界部署访问控制设备，启用访问控制功能 | 8 |
| 应能根据会话状态信息为数据流提供明确的允许/拒绝访问的能力，**控制粒度为端口级** |
| **应对进出网络的信息内容进行过滤，实现对应用层HTTP、FTP、TELNET、SMTP、POP3等协议命令级的控制** |
| **应在会话处于非活跃一定时间或会话结束后终止网络连接** |
| **应限制网络最大流量数及网络连接数** |
| **重要网段应采取技术手段防止地址欺骗** |
| 应按用户和系统之间的允许访问规则，决定允许或拒绝用户对受控系统进行资源访问，控制粒度为单个用户 |
| 应限制具有拨号访问权限的用户数量 |
| 安全审计 | 应对网络系统中的网络设备运行状况、网络流量、用户行为等进行日志记录； | 4 |
| 审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息。 |
| **应能够根据记录数据进行分析，并生成审计报表** |
| **应对审计记录进行保护，避免受到未预期的删除、修改或覆盖等** |
| 边界完整性  检查 | **应能够对非授权设备私自联到内部网络的行为进行检查，准确定出位置，并对其进行有效阻断** | 2 |
| 应能够对内部网络用户私自联到外部网络的行为进行检查，准确定出位置，**并对其进行有效阻断** |
| 入侵防范 | 应在网络边界处监视以下攻击行为：端口扫描、强力攻击、木马后门攻击、拒绝服务攻击、缓冲区溢出攻击、IP碎片攻击和网络蠕虫攻击等 | 2 |
| **当检测到攻击行为时，记录攻击源IP、攻击类型、攻击目的、攻击时间，在发生严重入侵事件时应提供报警** |
| 恶意代码  防范 | **应在网络边界处对恶意代码进行检测和清除** | 2 |
| **应维护恶意代码库的升级和检测系统的更新** |
| 网络设备  防护 | 应对登录网络设备的用户进行身份鉴别 | 8 |
| 应对网络设备的管理员登录地址进行限制 |
| 网络设备用户的标识应唯一 |
| **主要网络设备应对同一用户选择两种或两种以上组合的鉴别技术来进行身份鉴别** |
| 身份鉴别信息应具有不易被冒用的特点，口令应有复杂度要求并定期更换 |
| 应具有登录失败处理功能，可采取结束会话、限制非法登录次数和当网络登录连接超时自动退出等措施 |
| 当对网络设备进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听 |
| **应实现设备特权用户的权限分离** |
| 主机安全 | 身份鉴别 | 应对登录操作系统和数据库系统的用户进行身份标识和鉴别 | 6 |
| 操作系统和数据库系统管理用户身份标识应具有不易被冒用的特点，口令应有复杂度要求并定期更换 |
| 应启用登录失败处理功能，可采取结束会话、限制非法登录次数和自动退出等措施 |
| 当对服务器进行远程管理时，应采取必要措施，防止鉴别信息在网络传输过程中被窃听 |
| 应为操作系统和数据库系统的不同用户分配不同的用户名，确保用户名具有唯一性 |
| **应采用两种或两种以上组合的鉴别技术对管理用户进行身份鉴别** |
| 访问控制 | 应启用访问控制功能，依据安全策略控制用户对资源的访问 | 7 |
| **应根据管理用户的角色分配权限，实现管理用户的权限分离，仅授予管理用户所需的最小权限** |
| 应实现操作系统和数据库系统特权用户的权限分离 |
| 应限制默认帐户的访问权限，重命名系统默认帐户，修改这些帐户的默认口令 |
| 应及时删除多余的、过期的帐户、避免共享帐户的存在 |
| **应对重要信息资源设置敏感标记** |
| **应依据安全策略严格控制用户对有敏感标记重要信息资源的操作** |
| 安全审计 | 审计范围应覆盖到服务器和**重要客户端上**的每个操作系统用户和数据库用户 | 6 |
| 审计内容应包括重要用户行为、系统资源的异常使用和重要系统命令的使用等系统内重要的安全相关事件 |
| 审计记录应包括事件的日期、时间、类型、主体标识、客体标识和结果等 |
| **应能够根据记录数据进行分析，并生成审计报表** |
| **应保护审计进程，避免受到未预期的中断** |
| 应保护审计记录，避免受到未预期的删除、修改或覆盖等 |
| 剩余信息  保护 | **应保证操作系统和数据库系统用户的鉴别信息所在的存储空间，被释放或再分配给其他用户前得到完全清除，无论这些信息是存放在硬盘上还是在内存中** | 2 |
| **应确保系统内的文件、目录和数据库记录等资源所在的存储空间，被释放或重新分配给其他用户前得到完全清除** |
| 入侵防范 | **应能够检测到对重要服务器进行入侵的行为，能够记录入侵的源IP、攻击的类型、攻击的目的、攻击的时间，并在发生严重入侵事件时提供报警** | 3 |
| **应能够对重要程序的完整性进行检测，并在检测到完整性受到破坏后具有恢复的措施** |
| 操作系统应遵循最小安装的原则，仅安装需要的组件和应用程序，并通过设置升级服务器等方式保持系统补丁及时得到更新 |
| 恶意代码  防范 | 应安装防恶意代码软件，并及时更新防恶意代码软件版本和恶意代码库 | 3 |
| **主机防恶意代码产品应具有与网络防恶意代码产品不同的恶意代码库** |
| 应支持防恶意代码软件的统一管理 |
| 资源控制 | 应通过设定终端接入方式、网络地址范围等条件限制终端登录 | 5 |
| 应根据安全策略设置登录终端操作超时锁定 |
| **应对重要服务器进行监视，包括监视服务器的CPU、硬盘、内存、网络等资源的使用情况** |
| 应限制单个用户对系统资源的最大或最小使用限度 |
| **应能够对系统的服务水平降低到预先规定的最小值进行检测和报警** |
| 应用安全 | 身份鉴别 | 应提供专用的登录控制模块对登录用户进行身份标识和鉴别 | 5 |
| **应对同一用户采用两种或两种以上组合的鉴别技术实现用户身份鉴别** |
| 应提供用户身份标识唯一和鉴别信息复杂度检查功能，保证应用系统中不存在重复用户身份标识，身份鉴别信息不易被冒用 |
| 应提供登录失败处理功能，可采取结束会话、限制非法登录次数和自动退出等措施 |
| 应启用身份鉴别、用户身份标识唯一性检查、用户身份鉴别信息复杂度检查以及登录失败处理功能，并根据安全策略配置相关参数 |
| 访问控制 | 应提供访问控制功能，依据安全策略控制用户对文件、数据库表等客体的访问 | 6 |
| 访问控制的覆盖范围应包括与资源访问相关的主体、客体及它们之间的操作 |
| 应由授权主体配置访问控制策略，并严格限制默认帐户的访问权限 |
| 应授予不同帐户为完成各自承担任务所需的最小权限，并在它们之间形成相互制约的关系 |
| **应具有对重要信息资源设置敏感标记的功能** |
| **应依据安全策略严格控制用户对有敏感标记重要信息资源的操作** |
| 安全审计 | 应提供覆盖到每个用户的安全审计功能，对应用系统重要安全事件进行审计 | 4 |
| **应保证无法单独中断审计进程，**无法删除、修改或覆盖审计记录 |
| 审计记录的内容至少应包括事件日期、时间、发起者信息、类型、描述和结果等 |
| 应提供对审计记录数据进行统计、查询、分析及生成审计报表的功能 |
| 剩余信息  保护 | **应保证用户鉴别信息所在的存储空间被释放或再分配给其他用户前得到完全清除，无论这些信息是存放在硬盘上还是在内存中** | 2 |
| **应保证系统内的文件、目录和数据库记录等资源所在的存储空间被释放或重新分配给其他用户前得到完全清除** |
| 通信完整性 | 应采用**密码技术**保证通信过程中数据的完整性 | 1 |
| 通信保密性 | 在通信双方建立连接之前，应用系统应利用密码技术进行会话初始化验证 | 2 |
| 应对通信过程中的**整个报文或会话过程进行加密** |
| 抗抵赖 | **应具有在请求的情况下为数据原发者或接收者提供数据原发证据的功能** | 2 |
| **应具有在请求的情况下为数据原发者或接收者提供数据接收证据的功能** |
| 软件容错 | 应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的数据格式或长度符合系统设定要求 | 2 |
| **应提供自动保护功能，当故障发生时自动保护当前所有状态，保证系统能够进行恢复** |
| 资源控制 | 当应用系统的通信双方中的一方在一段时间内未作任何响应，另一方应能够自动结束会话 | 7 |
| 应能够对应用系统的最大并发会话连接数进行限制 |
| 应能够对单个帐户的多重并发会话进行限制 |
| **应能够对一个时间段内可能的并发会话连接数进行限制** |
| **应能够对一个访问帐户或一个请求进程占用的资源分配最大限额和最小限额** |
| **应能够对系统服务水平降低到预先规定的最小值进行检测和报警** |
| **应提供服务优先级设定功能，并在安装后根据安全策略设定访问帐户或请求进程的优先级，根据优先级分配系统资源** |
| 数据安全及备份  恢复 | 数据完整性 | 应能够检测到**系统管理数据**、鉴别信息和重要业务数据在传输过程中完整性受到破坏，**并在检测到完整性错误时采取必要的恢复措施** | 2 |
| **应能够检测到系统管理数据、鉴别信息和重要业务数据在存储过程中完整性受到破坏，并在检测到完整性错误时采取必要的恢复措施** |
| 数据保密性 | **应采用加密或其他有效措施实现系统管理数据、鉴别信息和重要业务数据传输保密性** | 2 |
| 应采用加密或其他保护措施实现**系统管理数据**、鉴别信息和**重要业务数据**存储保密性 |
| 备份和恢复 | **应提供本地数据备份与恢复功能，完全数据备份至少每天一次，备份介质场外存放** | 4 |
| **应提供异地数据备份功能，利用通信网络将关键数据定时批量传送至备用场地** |
| **应采用冗余技术设计网络拓扑结构，避免关键节点存在单点故障** |
| **应提供主要网络设备、通信线路和数据处理系统的硬件冗余，保证系统的高可用性** |
| 安全管理制度 | 管理制度 | 应制定信息安全工作的总体方针和安全策略，说明机构安全工作的总体目标、范围、原则和安全框架等 | 4 |
| 应对**安全管理活动中的各类管理内容**建立安全管理制度 |
| 应对安全管理人员或操作人员执行的重要管理操作建立操作规程 |
| **应形成由安全策略、管理制度、操作规程等构成的全面的信息安全管理制度体系** |
| 制定和发布 | 应指定或授权专门的部门或人员负责安全管理制度的制定 | 4 |
| **安全管理制度应具有统一的格式，并进行版本控制** |
| 应组织相关人员对制定的安全管理制度进行论证和审定 |
| **安全管理制度应通过正式、有效的方式发布** |
| **安全管理制度应注明发布范围，并对收发文进行登记** |
| 评审和修订 | **信息安全领导小组应负责定期组织相关部门和相关人员对安全管理制度体系的合理性和适用性进行审定** | 2 |
| **应定期或不定期对安全管理制度进行检查和审定**，对存在不足或需要改进的安全管理制度进行修订 |
| 安全管理机构 | 岗位设置 | 应**设立信息安全管理工作的职能部门**，设立安全主管、安全管理各个方面的负责人岗位，并定义各负责人的职责 | 4 |
| 应设立系统管理员、网络管理员、安全管理员等岗位，并定义各个工作岗位的职责 |
| **应成立指导和管理信息安全工作的委员会或领导小组，其最高领导由单位主管领导委任或授权** |
| **应制定文件明确安全管理机构各个部门和岗位的职责、分工和技能要求** |
| 人员配备 | 应配备一定数量的系统管理员、网络管理员、安全管理员等 | 3 |
| **应配备专职安全管理员，不可兼任** |
| **关键事务岗位应配备多人共同管理** |
| 授权和审批 | 应根据各个部门和岗位的职责明确**授权审批事项**、审批部门和批准人等 | 4 |
| **应针对系统变更、重要操作、物理访问和系统接入等事项建立审批程序，按照审批程序执行审批过程，对重要活动建立逐级审批制度** |
| **应定期审查审批事项，及时更新需授权和审批的项目、审批部门和审批人等信息** |
| **应记录审批过程并保存审批文档** |
| 沟通和合作 | 应加强各类管理人员之间、组织内部机构之间以及信息安全职能部门内部的合作与沟通，**定期或不定期召开协调会议，共同协作处理信息安全问题** | 5 |
| 应加强与兄弟单位、公安机关、电信公司的合作与沟通 |
| **应加强与供应商、业界专家、专业的安全公司、安全组织的合作与沟通** |
| **应建立外联单位联系列表，包括外联单位名称、合作内容、联系人和联系方式等信息** |
| **应聘请信息安全专家作为常年的安全顾问，指导信息安全建设，参与安全规划和安全评审等** |
| 审核和检查 | 安全管理员应负责定期进行安全检查，检查内容包括系统日常运行、系统漏洞和数据备份等情况 | 4 |
| **应由内部人员或上级单位定期进行全面安全检查，检查内容包括现有安全技术措施的有效性、安全配置与安全策略的一致性、安全管理制度的执行情况等** |
| **应制定安全检查表格实施安全检查，汇总安全检查数据，形成安全检查报告，并对安全检查结果进行通报** |
| **应制定安全审核和安全检查制度规范安全审核和安全检查工作，定期按照程序进行安全审核和安全检查活动** |
| 人员安全管理 | 人员录用 | 应指定或授权专门的部门或人员负责人员录用 | 4 |
| 应**严格**规范人员录用过程，对被录用人的身份、背景、专业资格和**资质**等进行审查，对其所具有的技术技能进行考核 |
| **应签署保密协议** |
| **应从内部人员中选拔从事关键岗位的人员，并签署岗位安全协议** |
| 人员离岗 | 应**严格**规范人员离岗过程，及时终止离岗员工的所有访问权限 | 3 |
| 应取回各种身份证件、钥匙、徽章等以及机构提供的软硬件设备 |
| 应办理严格的调离手续，**关键岗位人员离岗须承诺调离后的保密义务后方可离开** |
| 人员考核 | 应定期对各个岗位的人员进行安全技能及安全认知的考核 | 3 |
| **应对关键岗位的人员进行全面、严格的安全审查和技能考核** |
| **应对考核结果进行记录并保存** |
| 安全意识  教育和培训 | 应对各类人员进行安全意识教育、岗位技能培训和相关安全技术培训 | 4 |
| **应对安全责任和惩戒措施进行书面规定并告知相关人员，**对违反违背安全策略和规定的人员进行惩戒 |
| **应对定期安全教育和培训进行书面规定，针对不同岗位制定不同的培训计划，对信息安全基础知识、岗位操作规程等进行培训** |
| 应对安全教育和培训的情况和结果进行记录并归档保存 |
| 外部人员  管理 | 应确保在外部人员访问受控区域**前先提出书面申请**，批准后由专人全程陪同或监督，并登记备案 | 2 |
| **对外部人员允许访问的区域、系统、设备、信息等内容应进行书面的规定，并按照规定执行** |
| 系统建设管理 | 系统定级 | 应明确信息系统的边界和安全保护等级 | 4 |
| 应以书面的形式说明信息系统确定为某个安全保护等级的方法和理由 |
| **应组织相关部门和有关安全技术专家对信息系统定级结果的合理性和正确性进行论证和审定** |
| 应确保信息系统的定级结果经过相关部门的批准 |
| 安全方案  设计 | 应根据系统的安全保护等级选择基本安全措施，依据风险分析的结果补充和调整安全措施 | 5 |
| **应指定和授权专门的部门对信息系统的安全建设进行总体规划，制定近期和远期的安全建设工作计划** |
| **应根据信息系统的等级划分情况，统一考虑安全保障体系的总体安全策略、安全技术框架、安全管理策略、总体建设规划和详细设计方案，并形成配套文件** |
| 应组织相关部门和有关**安全技术专家对总体安全策略、安全技术框架、安全管理策略、总体建设规划、详细设计方案等相关配套文件**的合理性和正确性进行论证和审定，并且经过批准后，才能正式实施 |
| **应根据等级测评、安全评估的结果定期调整和修订总体安全策略、安全技术框架、安全管理策略、总体建设规划、详细设计方案等相关配套文件** |
| 产品采购和  使用 | 应确保安全产品采购和使用符合国家的有关规定 | 4 |
| 应确保密码产品采购和使用符合国家密码主管部门的要求 |
| 应指定或授权专门的部门负责产品的采购 |
| **应预先对产品进行选型测试，确定产品的候选范围，并定期审定和更新候选产品名单** |
| 自行软件  开发 | 应确保开发环境与实际运行环境物理分开，**开发人员和测试人员分离，测试数据和测试结果受到控制** | 5 |
| 应制定软件开发管理制度，明确说明开发过程的控制方法和人员行为准则 |
| **应制定代码编写安全规范，要求开发人员参照规范编写代码** |
| 应确保提供软件设计的相关文档和使用指南，并由专人负责保管 |
| **应确保对程序资源库的修改、更新、发布进行授权和批准** |
| 外包软件  开发 | 应根据开发要求检测软件质量 | 4 |
| 应确保提供软件设计的相关文档和使用指南 |
| 应在软件安装之前检测软件包中可能存在的恶意代码 |
| 应要求开发单位提供软件源代码，并审查软件中可能存在的后门 |
| 工程实施 | 应指定或授权专门的部门或人员负责工程实施过程的管理 | 3 |
| 应制定详细的工程实施方案控制实施过程，**并要求工程实施单位能正式地执行安全工程过程** |
| **应制定工程实施方面的管理制度，明确说明实施过程的控制方法和人员行为准则** |
| 测试验收 | 应**委托公正的第三方测试单位**对系统进行安全性测试，**并出具安全性测试报告** | 5 |
| 在测试验收前应根据设计方案或合同要求等制订测试验收方案，在测试验收过程中应详细记录测试验收结果，并形成测试验收报告 |
| 应对系统测试验收的控制方法和人员行为准则进行书面规定 |
| **应指定或授权专门的部门负责系统测试验收的管理，并按照管理规定的要求完成系统测试验收工作** |
| **应组织相关部门和相关人员对系统测试验收报告进行审定，并签字确认** |
| 系统交付 | 应制定**详细的**系统交付清单，并根据交付清单对所交接的设备、软件和文档等进行清点 | 5 |
| 应对负责系统运行维护的技术人员进行相应的技能培训 |
| 应确保提供系统建设过程中的文档和指导用户进行系统运行维护的文档 |
| **应对系统交付的控制方法和人员行为准则进行书面规定** |
| **应指定或授权专门的部门负责系统交付的管理工作，并按照管理规定的要求完成系统交付工作** |
| 系统备案 | **应指定专门的部门或人员负责管理系统定级的相关材料，并控制这些材料的使用** | 3 |
| **应将系统等级及相关材料报系统主管部门备案** |
| **应将系统等级及其他要求的备案材料报相应公安机关备案** |
| 等级测评 | **在系统运行过程中，应至少每年对系统进行一次等级测评，发现不符合相应等级保护标准要求的及时整改** | 4 |
| **应在系统发生变更时及时对系统进行等级测评，发现级别发生变化的及时调整级别并进行安全改造，发现不符合相应等级保护标准要求的及时整改** |
| **应选择具有国家相关技术资质和安全资质的测评单位进行等级测评** |
| **应指定或授权专门的部门或人员负责等级测评的管理** |
| 安全服务商  的选择 | 应确保安全服务商的选择符合国家的有关规定 | 3 |
| 应与选定的安全服务商签订与安全相关的协议，明确约定相关责任 |
| 应确保选定的安全服务商提供技术支持和服务承诺，必要的与其签订服务合同 |
| 系统运维管理 | 环境管理 | 应指定专门的部门或人员定期对机房供配电、空调、温湿度控制等设施进行维护管理 | 4 |
| **应指定部门负责机房安全**，并配备机房安全管理人员，对机房的出入、服务器的开机或关机等工作进行管理 |
| 应建立机房安全管理制度，对有关机房物理访问，物品带进、带出机房和机房环境安全等方面的管理作出规定 |
| 应加强对办公环境的保密性管理，规范办公环境人员行为，包括工作人员调离办公室应立即交还该办公室钥匙、不在办公区接待来访人员、**工作人员离开座位应确保终端计算机退出登录状态和桌面上没有包含敏感信息的纸档文件等** |
| 资产管理 | 应编制与信息系统相关的资产清单，包括资产责任部门、重要程度和所处位置等内容 | 4 |
| 应建立资产安全管理制度，规定信息系统资产管理的责任人员或责任部门，并规范资产管理和使用的行为 |
| **应根据资产的重要程度对资产进行标识管理，根据资产的价值选择相应的管理措施** |
| **应对信息分类与标识方法作出规定，并对信息的使用、传输和存储等进行规范化管理** |
| 介质管理 | **应建立介质安全管理制度，对介质的存放环境、使用、维护和销毁等方面作出规定** | 6 |
| 应确保介质存放在安全的环境中，对各类介质进行控制和保护，并实行存储环境专人管理 |
| 应**对介质在物理传输过程中的人员选择、打包、交付等情况进行控制**，对介质归档和查询等进行登记记录，并根据存档介质的目录清单定期盘点 |
| 应对存储介质**的使用过程**、送出维修以及销毁等进行严格的管理，**对带出工作环境的存储介质进行内容加密和监控管理**，对送出维修或销毁的介质应首先清除介质中的敏感数据，**对保密性较高的存储介质未经批准不得自行销毁** |
| **应根据数据备份的需要对某些介质实行异地存储，存储地的环境要求和管理方法应与本地相同** |
| **应对重要介质中的数据和软件采取加密存储**，并根据所承载数据和软件的重要程度对介质进行分类和标识管理 |
| 设备管理 | 应对信息系统相关的各种设备（包括备份和冗余设备）、线路等指定专门的部门或人员定期进行维护管理 | 5 |
| 应建立基于申报、审批和专人负责的设备安全管理制度，对信息系统的各种软硬件设备的选型、采购、发放和领用等过程进行规范化管理 |
| **应建立配套设施、软硬件维护方面的管理制度，对其维护进行有效的管理，包括明确维护人员的责任、涉外维修和服务的审批、维修过程的监督控制等** |
| 应对终端计算机、工作站、便携机、系统和网络等设备的操作和使用进行规范化管理，按操作规程实现关键设备（包括备份和冗余设备）的启动/停止、加电/断电等操作 |
| 应确保信息处理设备必须经过审批才能带离机房或办公地点 |
| 监控管理和安全管理  中心 | **应对通信线路、主机、网络设备和应用软件的运行状况、网络流量、用户行为等进行监测和报警，形成记录并妥善保存** | 3 |
| **应组织相关人员定期对监测和报警记录进行分析、评审，发现可疑行为，形成分析报告，并采取必要的应对措施** |
| **应建立安全管理中心，对设备状态、恶意代码、补丁升级、安全审计等安全相关事项进行集中管理** |
| 网络安全  管理 | 应指定人员对网络进行管理，负责运行日志、网络监控记录的日常维护和报警信息分析和处理工作 | 8 |
| 应建立网络安全管理制度，对网络安全配置、日志保存时间、安全策略、升级与打补丁、口令更新周期等方面作出规定 |
| 应根据厂家提供的软件升级版本对网络设备进行更新，并在更新前对现有的重要文件进行备份 |
| 应定期对网络系统进行漏洞扫描，对发现的网络系统安全漏洞进行及时的修补 |
| **应实现设备的最小服务配置**，并对配置文件进行定期离线备份 |
| 应保证所有与外部系统的连接均得到授权和批准 |
| **应依据安全策略允许或者拒绝便携式和移动式设备的网络接入** |
| **应定期检查违反规定拨号上网或其他违反网络安全策略的行为** |
| 系统安全  管理 | 应根据业务需求和系统安全分析确定系统的访问控制策略 | 7 |
| 应定期进行漏洞扫描，对发现的系统安全漏洞及时进行修补 |
| 应安装系统的最新补丁程序，在安装系统补丁前，应首先在测试环境中测试通过，并对重要文件进行备份后，方可实施系统补丁程序的安装 |
| 应建立系统安全管理制度，对系统安全策略、安全配置、日志管理和日常操作流程等方面作出规定 |
| **应指定专人对系统进行管理，划分系统管理员角色，明确各个角色的权限、责任和风险，权限设定应当遵循最小授权原则** |
| 应依据操作手册对系统进行维护，详细记录操作日志，包括重要的日常操作、运行维护记录、参数的设置和修改等内容，严禁进行未经授权的操作 |
| 应定期对运行日志和审计数据进行分析，以便及时发现异常行为 |
| 恶意代码  防范管理 | 应提高所有用户的防病毒意识，告知及时升级防病毒软件，在读取移动存储设备上的数据以及网络上接收文件或邮件之前，先进行病毒检查，对外来计算机或存储设备接入网络系统之前也应进行病毒检查 | 4 |
| 应指定专人对网络和主机进行恶意代码检测并保存检测记录 |
| 应对防恶意代码软件的授权使用、恶意代码库升级、定期汇报等作出明确规定 |
| **应定期检查信息系统内各种产品的恶意代码库的升级情况并进行记录，对主机防病毒产品、防病毒网关和邮件防病毒网关上截获的危险病毒或恶意代码进行及时分析处理，并形成书面的报表和总结汇报** |
| 密码管理 | **应建立密码使用管理制度**，使用符合国家密码管理规定的密码技术和产品 | 1 |
| 变更管理 | 应确认系统中要发生的重要变更，并制定相应的变更方案 | 4 |
| **应建立变更管理制度**，系统发生变更前，向主管领导申请，变更和变更方案经过评审、审批后方可实施变更，并在实施后将变更情况向相关人员通告 |
| **应建立变更控制的申报和审批文件化程序，对变更影响进行分析并文档化，记录变更实施过程，并妥善保存所有文档和记录** |
| **应建立中止变更并从失败变更中恢复的文件化程序，明确过程控制方法和人员职责，必要时对恢复过程进行演练** |
| 备份与恢复  管理 | 应识别需要定期备份的重要业务信息、系统数据及软件系统等 | 5 |
| **应建立备份与恢复管理相关的安全管理制度，**对备份信息的备份方式、备份频度、存储介质和保存期等进行规范 |
| 应根据数据的重要性及其对系统运行的影响，制定数据的备份策略和恢复策略，备份策略指明备份数据的放置场所、文件命名规则、介质替换频率和数据离站运输方法 |
| **应建立控制数据备份和恢复过程的程序，对备份过程进行记录，所有文件和记录应妥善保存** |
| **应定期执行恢复程序，检查和测试备份介质的有效性，确保可以在恢复程序规定的时间内完成备份的恢复** |
| 安全事件  处置 | 应报告所发现的安全弱点和可疑事件，但任何情况下用户均不应尝试验证弱点 | 6 |
| 应制定安全事件报告和处置管理制度，明确安全事件类型，规定安全事件的现场处理、事件报告和后期恢复的管理职责 |
| 应根据国家相关管理部门对计算机安全事件等级划分方法和安全事件对本系统产生的影响，对本系统计算机安全事件进行等级划分 |
| **应制定安全事件报告和响应处理程序，确定事件的报告流程，响应和处置的范围、程度，以及处理方法等** |
| **应在安全事件报告和响应处理过程中，分析和鉴定事件产生的原因，收集证据，记录处理过程，总结经验教训，制定防止再次发生的补救措施，过程形成的所有文件和记录均应妥善保存** |
| **对造成系统中断和造成信息泄密的安全事件应采用不同的处理程序和报告程序** |
| 应急预案  管理 | 应在统一的应急预案框架下制定不同事件的应急预案，应急预案框架应包括启动应急预案的条件、应急处理流程、系统恢复流程、事后教育和培训等内容 | 5 |
| **应从人力、设备、技术和财务等方面确保应急预案的执行有足够的资源保障** |
| 应对系统相关的人员进行应急预案培训，应急预案的培训应至少每年举办一次 |
| **应定期对应急预案进行演练，根据不同的应急恢复内容，确定演练的周期** |
| **应规定应急预案需要定期审查和根据实际情况更新的内容，并按照执行** |

## 需求分析

根据前期调研，结合以上风险分析，初步分析当前存在的主要需求，具体如下：

（1）信息系统等级保护测评。依据国家信息安全等级保护制度规定，根据等保测评相关标准，从安全技术与安全管理两大项10个方面，对信息系统安全等级保护状况进行全面测试与综合评估，找出信息系统可能存在的每个安全问题与弱点，进行相应的整改，然后开展最终的验收测评，并提交符合国家信息安全等级保护主管部门要求的验收测评报告。

（2）网络结构的优化。根据对信息系统网络情况的初步分析，需要对现有网络结构进行优化，增加核心交换机，提高处理业务数据的可靠性、性能，提高信息系统的可扩展性。

（3）边界安全防护。针对服务器边界部署访问控制、入侵防范设备进行安全防护。建立起信息系统准入控制机制，控制非法外联内联。

（4）网络环境的安全防护。建立起安全审计机制，汇集各类安全事件和设备日志，进行事件追踪、事件源定位以定位恶意人员位置，尽早发现网络、主机、操作系统、中间件、数据库、业务应用、机房等IT设施的异常并实时报警以便迅速处置。

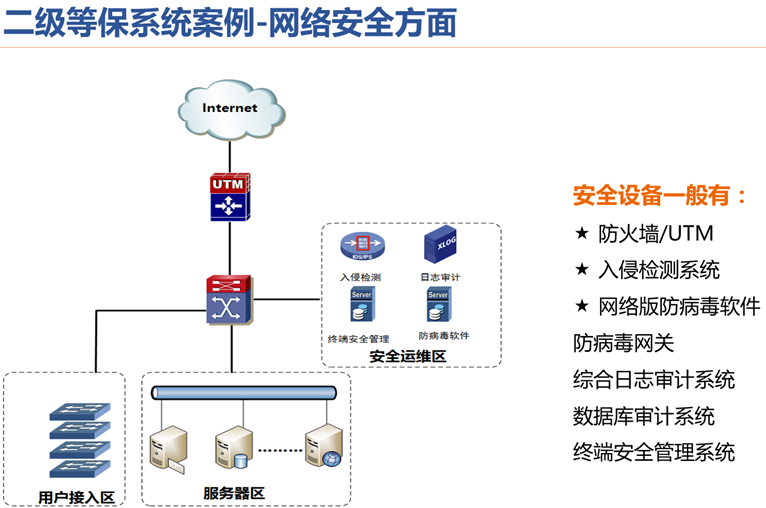
（5）主机安全防护。对应用服务器、办公终端和业务终端等进行统一的、集中的防恶意代码、行为进行管理。

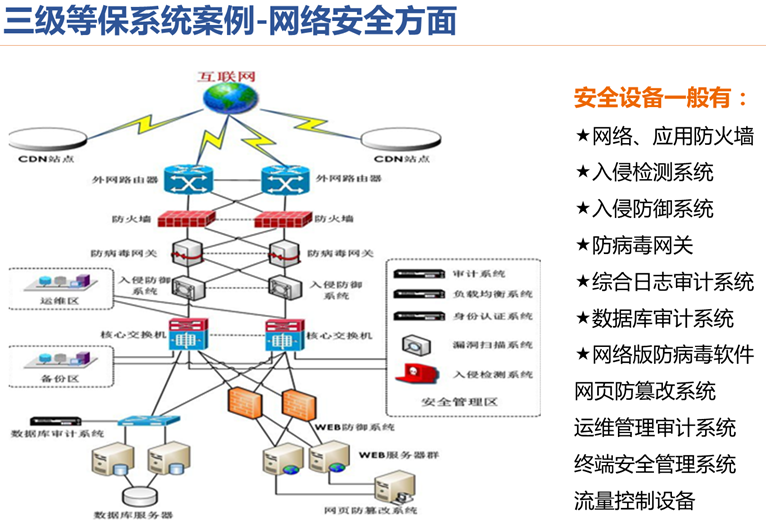
# 方案总体规划

## 规划目标

根据信息安全等级保护X级系统相关要求，结合XXXXXXXXXX初步调研情况，针对重点区域规划相对应的安全产品，根据等级保护制度要求及《网络安全法》的相关要求，针对部分需要进行安全加固和运行维护的，提出应该开展的安全服务。使其网络安全产品部署、安全服务上基本满足等级保护X级要求。

## 整改产品规划





网络结构优化

核心交换机

根据信息安全等级保护基本要求：应保证主要网络设备的业务处理能力具备冗余空间，满足业务高峰期需要；应保证网络各个部分的带宽满足业务高峰期需要；应采用冗余技术设计网络拓扑结构，避免关键节点存在单点故障；应提供主要网络设备、通信线路和数据处理系统的硬件冗余，保证系统的高可用性。

建议将目前处于核心区域的XX 型号防火墙替换为核心交换机，并冗余部署，保证系统的高可用性，提升业务处理能力。

* **基本参数**

|  |  |  |
| --- | --- | --- |
| 产品类型 | 三层核心交换机 | |
| 接入模式 | 串联 | |
| 部署位置 | 部署在核心区域 | |
| 主要功能 | 访问控制 | 1、支持vlan划分。 2、支持路由功能。  3、支持动态端口协议的细粒度访问控制功能。 4、可实现静态或自动的IP/MAC绑定。 |
| 流量控制 | 1、支持常规QoS带宽控制。 |
| 管理配置 | 系统管理 | 1、支持远程SSH和串口命令行配置。 2、支持数字证书和电子钥匙两种管理员认证方式（可选） 3、支持管理员权限分级。 4、支持设备特权用户的权限分离。 5、支持对管理员登录IP地址的限制。 6、支持身份鉴别安全策略，支持但不限于如密码长度、复杂度、密码历史、登录失败限制、有效期等策略控制。 |
| 日志报警 | 1、支持设备内存储和外发专用事件分析服务器两种日志管理方式。 2、支持分级报警，支持但不限于SNMP Trap、邮件和短信等报警方式。 3、支持生成日志报表功能。（可选） |
| 资质需求 | 公安许可需求 | 具备公安部颁发的《计算机信息系统安全专用产品销售许可证》 |

边界安全防护

服务器边界防火墙

根据信息安全等级保护基本要求：应在网络边界部署访问控制设备，启用访问控制功能。

建议在服务器边界部署1台防火墙，对服务器边界进出的数据进行过滤。实现对服务器边界的访问控制和安全防护。

* **基本参数**

|  |  |
| --- | --- |
| 产品类型 | 防火墙 |
| 接入模式 | 直联 |
| 部署位置 | 部署在服务器边界区域 |
| ▲硬件架构 | 采用非X86 64位多核高性能处理器和高速存储器  主控模块内存≥4G;；高度≤2U盒式设备 |
| ▲产品性能配置要求 | 千兆光口≥8；个千兆电口≥16；扩展槽≥2；硬盘槽位≥1，支持硬盘容量≥500G（投标时须提供规格截图，并原厂盖章） |
| 最大并发连接数≥400万  IPSec VPN并发连接数≥2000  每秒新建连接数≥50K  整机大包吞吐量≥2.5Gbps  整机混合包吞吐量≥2G  整机小包吞吐量≥800M  整机DPI深度防御吞吐量≥2G  3DES加密≥2G  AES256加密≥2G  实配内置固化交流电源≥2 |
| ▲可靠性要求 | 支持双机虚拟化堆叠技术（非VRRP），融合后可统一管理配置并实现负载分担和业务备份，（投标时须提供配置截图，并原厂盖章） |
| 基本功能 | 支持安全区域管理，可基于接口、VLAN划分安全区域ASPF状态检查 |
| 支持FTP、HTTP、SMTP、RTSP、H323协议簇的状态报文过滤，支持时间段安全策略设置。 |
| 支持基于用于、应用的多维安全策略配置，并提供一体化安全策略配置模板（单条策略融合IPS、AV、ACG等多业务），（投标时须提供配置截图，并原厂盖章） |
| ▲支持基于CPU、内存等硬件划分资源的完全独立式虚拟化,可分配吞吐量、新建、并发，虚拟防火墙数量≥16个（投标时须提供配置截图，并原厂盖章） |
| 免费支持高性能IPSec、L2TP、GRE VPN功能  能够实现与L2TP over IPSec与安卓、ISO系统自带VPN组件对接  支持高性能SSL VPN功能，最大并发可扩展≥1000，实配125个SSL VPN用户授权 |
| 支持应用层防护：入侵防御、带宽管理，（投标时须提供配置截图，并原厂盖章） |
| 支持URL过滤、反垃圾邮件及敏感信息防泄漏功能 |
| ▲支持链路负载均衡功能、服务器负责均衡功能，（投标时须提供配置截图，并原厂盖章） |
| 支持IPv6：IPV6状态防火墙、IPV6动态路由协议、IPV6攻击防范、IPV6虚拟防火墙、IPV6管理、NAT64\DS-LITE等过渡技术，投标时须提供配置截图，并原厂盖章） |
| 支持静态路由、RIP v1/2、OSPF、ISIS、BGP、策略路由等 |
| 能够防范DOS/DDOS攻击：  Land、Smurf、Fraggle、WinNuke、Ping of Death、Tear Drop、IP Spoofing、SYN Flood、ICMP Flood、UDP Flood、HTTP Flood（cc）攻击、ARP欺骗、TCP报文标志位不合法、超大ICMP报文、地址扫描的防范、端口扫描的防范 |
| ★资质证明及其它要求 | 提供中华人民共和国公安部的《计算机信息系统安全专用产品销售许可证》，投标时须提供有效证书的复印件。  具有中国信息安全认证中心ISCCC颁发的《中国国家信息安全产品认证证书》，投标时须提供有效证书的复印件。  考虑管理的兼容性，所有的安全设备（日志审计系统、入侵检测系统、防火墙、核心交换机）为同一品牌 |

入侵检测系统

根据信息安全等级保护基本要求：应在网络边界处监视以下攻击行为：端口扫描、强力攻击、木马后门攻击、拒绝服务攻击、缓冲区溢出攻击、IP碎片攻击和网络蠕虫攻击等.

新增1台入侵检测设备，旁路部署。入侵检测的功能和优点主要体现在以下几个方面：

1. 能在网络中基于内容的检测，能够在对看似合法访问的信息中发现攻击的信息（比如隐藏在URL中的攻击行为），并做出相应的处理；
2. 能够对网络的入侵行为进行详细完整的记录，为以后的调查取证提供了有力的保障；对发现的入侵行为有多种灵活的处理方式，比如：中断非法连接、发出电子邮件或传呼警告等等；
3. 不仅可以检测来自外部的攻击，还可以检测来自内部的相互攻击。

* **基本参数**

|  |  |  |
| --- | --- | --- |
| 产品类型 | IDS（入侵检测系统） | |
| 接入模式 | 旁路 | |
| 部署位置 | 部署在核心区域 | |
| 主要功能 | 协议分析支持 | 1、支持IP碎片重组、TCP流重组、流量状态追踪，采用基于行为分析的检测技术。  2、全面检测100种以上的应用层协议包括不限于：  AUTH,DNS,FINGER,FTP,HTTP,ICMP,IMAP,IP,IRC,MSRPC,NETBIOSSSN,NFS,NNTP,POP3,QQ,RIP,SMTP,SNMP,SUNRPC,TCP,TDS,TELNET,TFTP,TNS,UDP,WHOIS |
| 攻击特征库 | 1、支持8000条以上的安全事件库，包括不限于能够检测常见端口扫描攻击、木马后门、拒绝服务攻击、蠕虫、病毒、洛伊木马、p2p、IM、网络游戏以及其他违规行为、缓冲溢出、远程服务攻击、邮件服务器攻击、远程登陆攻击、GI访问攻击、IIS服务器攻击等。 2、系统携带的攻击特征库获得CVE兼容性认证。 3、3年的特征库升级授权。 |
| 攻击检测类别 | 1、支持对网络病毒、蠕虫、间谍软件、木马后门、刺探扫描、暴力破解等恶意流量的实时检测和报警，具备基于原理的WEB漏洞检测能力，能够有效检测SQL注入、跨站脚本等针对重点服务器的攻击行为。 2、支持自定义入侵行为和应用软件特征，可根据需求定制对其它流量的检测规则。 |
| 响应能力 | 提供丰富的响应方式，包括不限于：丢弃数据包、阻断会话、邮件报警、短信报警、控制台显示、日志数据库记录等 。 |
| 第三方设备互动 | 1、支持与主流防火墙进行联动阻断入侵者。 2、提供标准snmp 和syslog接口，可接受第三方安全管理平台的事件管理。 |
| 管理配置 | 系统管理 | 1、支持安全且友好的Web（HTTPS）图形界面配置，以简单、直观的方式完成策略配置、警报查询、攻击响应、集中管理等各种任务。2、支持远程SSH和串口命令行配置。  3、支持数字证书和电子钥匙两种管理员认证方式。  4、支持管理员权限分级。  5、支持设备特权用户的权限分离。 6、支持对管理员登录IP地址的限制。 7、支持身份鉴别安全策略，支持但不限于如密码长度、复杂度、密码历史、登录失败限制、有效期等策略控制。 |
| 日志管理 | 1、支持实时的日志归并功能，可以根据需要，按照源/目的IP/MAC地址、事件类型等信息，对告警日志执行任意粒度的归并。  2、日志信息的存储支持主流数据库，以及第三方syslog服务器。 3、提供基于时间、IP地址、事件类别等条件的日志检索功能，具备日志备份、清除和恢复功能。 |
| 报表系统 | 1、提供丰富的报表功能，支持用户自定义报表模版，能够按照用户需求生成各种风格的统计报表。 2、支持将生成的报表以PDF/html/word、excel等通用格式输出。 |
| 安全分析 | 1、能根据安全类型、流行程度、事件级别等条件自定义哪些事件需要在界面展示，除IP地址以外，能直接显示某个应用系统，某个操作系统是否收到事件影响，实现快速准确定位。  2、能根据事件发起者的威胁能力级别，对事件进行分类，展现网络中是否存在高级黑客行为。  3、提供事件确认功能，对威胁事件的处理方式及状态进行人工智能辅助确认，可根据源地址、目的地址、事件类型等参数，对智能批量事件处理做逻辑设置，便于在大量事件爆发环境中的管理。  4、能根据事件发起者威胁能力水平、业务系统名称、操作系统名称等因素导出报表，直观展示网络威胁状况。 |
| 资质需求 | 公安许可需求 | 具备公安部颁发的《计算机信息系统安全专用产品销售许可证》 |

网络准入控制系统

根据信息安全等级保护基本要求：应能够对非授权设备私自联到内部网络的行为进行检查，准确定出位置，并对其进行有效阻断。

建议部署1台网络准入控制系统，解决系统的合规性要求，达到“违规不入网、入网必合规”的管理规范，审计终端用户行为，提供高效的网络准入防护体系。

* **基本参数**

|  |  |  |
| --- | --- | --- |
| 产品类型 | 网络准入控制 | |
| 接入模式 | 旁路 | |
| 部署位置 | 部署在核心区域 | |
| 主要功能 | 边界控制管理 | 帮助用户快速实现内网边界规划，实现基于接入层边界的控制和基于重要资源边界的控制。 |
| 人员认证管理 | 提供本地用户名/密码、Email、Radius、LDAP、AD域、短信、生物指纹等其他第三方认证方式 |
| 设备规范管理 | 提供多项内网安全要素，包括：通用规范和行业特征规范   1. 设备识别，根据IP、MAC、操作系统、硬盘ID、系统指纹等特征完整的识别接入设备形态，帮助管理者区分内部设备与外部设备 2. 用户认证，提供管理者基于用户的角色管理，赋予不同用户不同的访问权限、所使用设备的安全配置要素及网络行为准则 3. 防病毒软件健康保障，针对主流杀毒软件，基于用户规划边界，确保终端设备接入边界时检测漏装、不更新病毒库或杀毒引擎等，强制管理终端设备的安全配置 4. 系统补丁，提供适合用户的补丁分级管理机制，确保安装的补丁具有高稳定性和安全针对性 |
| 操作行为管理 | 1. 对用户各种操作的监控和响应，包括IP更改、违规软件使用、必须安装软件随意卸载、网络访问操作、安全检查违规 2. 计算机设备状态的监控和响应，包括资产变更、系统环境变更、入网\出网状态变更、开\关机状态变更 3. 计算机设备的统一维护管理，包括类别管理、资产信息管理、软件分发、服务管理、资产探测 4. 违规外联管控，包括终端外联行为检测、终端外联行为阻断、外联行为记录、违规外联报警 |
| 视觉报表管理 | 1. 基于网络管理的整体视图，获取基础设施资产概况、物理分布、连接状况、地址分配、所有物理位置的接入设备状况 2. 基于端口的空间定位，展现所有网络设备的各个端口的运行状态 3. 事件\时间交互定位，将所有事件（入网、出网、上线、下线、认证、评估、检测等），对时间进行事件定位或通过事件查询时间报表 |
| 管理配置 | 准入控制 | 支持包括802.1x、PBR、MVG、Bridge等多种准入控制技术 |
| 部署管理 | 1. 集中式部署 2. 分布式部署 |
| 报警 | 支持邮件提醒、手机短信报警功能 |
| 资质需求 | 公安许可需求 | 具备公安部颁发的《计算机信息系统安全专用产品销售许可证》 |

网络环境安全防护

安全管理中心SOC

根据信息安全等级保护基本要求：应对通信线路、主机、网络设备和应用软件的运行状况、网络流量、用户行为等进行监测和报警，形成记录并妥善保存；应组织相关人员定期对监测和报警记录进行分析、评审，发现可疑行为，形成分析报告，并采取必要的应对措施；应建立安全管理中心，对设备状态、恶意代码、补丁升级、安全审计等安全相关事项进行集中管理。

建议在系统中部署1套安全管理中心SOC，全面采集系统中的安全设备、网络设备、服务器系统、应用软件和数据库的安全告警、性能告警、配置变更及故障报警等，从资产管理角度出发进行关联风险分析，实时监控系统服务的所有核心服务器及设备的关键运行指标，实现运维监控、态势分析、配置维护的全部功能。从而满足等级保护对于监控管理和安全管理中心的要求，满足《网络安全法》对于日志留存、安全事件监测预警的要求。主要应具备的基本功能：

**面向业务的统一安全管理**

反映业务支撑系统的资产构成，并自动构建业务健康指标体系，从业务的性能与可用性、业务的脆弱性和业务的威胁三个维度计算业务的健康度，从业务的角度去分析业务可用性、业务安全事件和业务告警。

**全面的日志采集**

可以通过多种方式来收集设备和业务系统的日志，例如Syslog、SNMP Trap、FTP、OPSEC LEA、NETBIOS、ODBC、WMI、Shell脚本、Web Service等等。

**智能化安全事件关联分析**

借助智能事件关联分析引擎，系统能够实时不间断地对所有范式化后的日志流进行安全事件关联分析。提供基于规则的关联分析、基于情境的关联分析和基于行为的关联分析，并提供可视化安全事件分析视图，结合威胁情报，更好的分析及发现安全问题。

**主动化的预警管理**

可以通过预警管理功能发布内部及外部的早期预警信息，并与网络中的IP资产进行关联，分析出可能受影响的资产，提前了解业务系统可能遭受的攻击和潜在的安全隐患。

**主动化的网络威胁情报利用**

提供主动化的威胁情报采集，通过采集实时威胁情报，结合规则关联和观察列表等分析方式，使安全管理人员及时发现来自已发现的外部攻击源的威胁。

**指标化宏观态势感知**

针对系统收集到的海量安全事件，系统借助地址熵分析、热点分析、威胁态势分析、KPI分析等数据挖掘技术，帮助管理员从宏观层面把握整体安全态势，对重大威胁进行识别、定位、预测和跟踪。

**多样的安全响应管理**

完善的响应管理功能，能够根据用户设定的各种触发条件，通过多种方式（例如邮件、短信、声音、SNMP Trap、即时消息、工单等）通知用户，并触发响应处理流程，直至跟踪到问题处理完毕，从而实现安全事件的闭环管理。

**丰富灵活的报表报告**

出具报表报告是安全管理平台的重要用途，系统内置了丰富的报表模板，包括统计报表、明细报表、综合审计报告，审计人员可以根据需要生成不同的报表。系统内置报表生成调度器，可以定时自动生成日报、周报、月报、季报、年报，并支持以邮件等方式自动投递，支持以PDF、Excel、Word等格式导出，支持打印。

**一体化安全管控界面**

提供一体化安全管控功能界面，为不同层级的用户提供了多视角、多层次的管理视图。

运维管理审计系统（堡垒机）

根据等级保护对于网络设备防护、身份鉴别、安全审计等相关要求，建议在XXXXXXXXXX中部署一台运维管理审计系统，通过集中管理模式，实现对运维操作过程的用户帐号管理、访问控制、权限控制和事后操作审计的集中管理，从而达到对运维操作过程的事先主动预防、事中实时控制和事后审计回放的目的，发现并及时制止用户的误操作、违规访问或者可疑行为，最大程度的降低运维操作风险。

* **基本参数**

|  |  |  |
| --- | --- | --- |
| 产品类型 | 运维管理审计系统（堡垒机） | |
| 接入模式 | 旁路 | |
| 部署位置 | 部署在核心区域 | |
| 主要功能 | 身份认证及访问授权 | 1、支持多种认证方式：本地密码认证、RSA动态口令认证、安盟动态口令认证、第三方RADIUS协议服务系统认证、LDAP认证、AD域认证、短信认证及U-KEY认证。 2、内置配置管理员、密码管理员、审计管理员、系统管理员、系统审计员、普通用户等管理角色。 3、支持单点登录功能，使用人员无需知道目标服务器帐号及密码，无需进行二次登录认证。 4、支持基于用户（用户组）、目标设备（设备组）、系统帐号、协议类型、生效时间范围、IP地址限制等设置访问控制策略。 5、支持审批模式：运维用户访问特定的服务器设备必须经过管理员的临时审批授权才能进行，否则无法登录。  6、支持预处理命令设置。  7、支持设定会话连接单位时间内空闲无操作，连接自动断开。 8、支持运维用户多次登录失败自动锁定账号功能。 |
| Web访问方式 | 1、 Web访问方式:通过系统的Web页面调用JAVA或activeX控件的方式直接访问服务器或通过WEB页面调用本地工具直接访问服务器。 2、多种类浏览器支持：IE（6-11）、firefox、chrome、safari。 3、支持设定窗口颜色、保存屏幕内容、打印屏幕内容、复制粘贴等功能。 |
| 客户端访问方式 | 1、客户端访问方式：通过管理员常用的客户端(如SecureCRT、PUTTY、Mstsc、PLsql、SQLplus等)访问。  2、支持客户端(SecureCRT、putty)clone session功能。 3、支持secure shell client软件中直接调用sftp功能。 |
| 支持协议 | 1、字符型远程操作协议：SSH(V1、V2)、TELNET、RLOGIN、AS400。  2、图形化远程操作协议：RDP、VNC、X11。 3、文件传输协议：FTP、SFTP。 4、数据库远程操作协议：支持ORACLE、MSSQL、Sybase、Mysql、DB2数据库远程访问协议审计。 |
| 操作行为记录 | 1、针对SSH、Telnet、Rlogin、FTP/SFTP、数据库操作进行记录及审计；记录发生时间、发生地址、服务端IP、客户端IP、操作指令、返回信息、操作备注、客户端端口、服务器端口、运维用户帐号、运维用户姓名、审批用户帐号、审批用户姓名、服务器用户名等信息。 2、针对RDP、VNC、X11等图形终端操作的连接情况进行记录及审计；记录发生时间、发生地址、服务端IP、客户端IP、操作指令、返回信息、操作备注、客户端端口、服务器端口、运维用户帐号、运维用户姓名、审批用户帐号、审批用户姓名、服务器用户名等信息。 |
| 会话过程回放 | 1、支持以线视频回放方式重现维护人员对服务器的所有操作过程，无须在客户端安装播放客户端软件。  2、支持倍速/低速播放、拖动、暂停、停止、重新播放等播放控制操作。  3、支持从特定操作指令开始进行定位回放。 4、支持空闲时间过滤。 |
| 事件监控 | 1、对于正在进行的运维操作会话，支持实时监控，支持手工切断实时会话。 2、支持Vi、aix下smit、rhel下setup等图形或菜单操作进行全程同步监控。 3、应支持监控审计运维用户在什么时间、什么IP登录了什么资产，什么时间登出，并记录完整的从登录到退出的整个过程。 4、支持审计记录的真实回放，操作回放需在WEB管理界面独立完成。 5、支持rdp协议的键盘记录、文字识别、及回放显示。 |
| 管理配置 | 系统管理 | 1、B/S方式，采用HTTPS方式远程安全管理，无需安装管理客户端。 2、支持管理员权限分级。  3、支持对管理员登录IP地址的限制。  4、支持身份鉴别安全策略，支持但不限于如密码长度、复杂度、密码历史、登录失败限制、有效期等策略控制。 |
| 报表分析功能 | 1、支持根据查询结果直接定位视频文件，回放历史会话。 2、系统内置多种运行维护报表模板。  3、支持以html、CSV或PDF方式生成并导出报表。 4、支持管理员自定义审计报表。  5、支持以日报、周报、月报的方式自动生成周期性报表，并自动发送至指定邮箱。 |
| 查询分析功能 | 1、支持快速查询和高级查询功能。  2、支持同一次会话中的指令关联查询，显示会话中所有操作指令。 |
| 资质需求 | 公安许可需求 | 具备公安部颁发的《计算机信息系统安全专用产品销售许可证》 |

安全态势感知平台

态势感知是一种基于环境的、动态、整体地洞悉安全风险的能力，是以安全大数据为基础，从全局视角提升对安全威胁的发现识别、理解分析、响应处置能力的一种方式，最终是为了决策与行动，是安全能力的落地。满足《网络安全法》中针对安全监测预警的相关要求。

**检测：**提供网络安全持续监控能力，及时发现各种攻击威胁与异常，特别是针对性攻击。

**分析、响应：**建立威胁可视化及分析能力，对威胁的影响范围、攻击路径、目的、手段进行快速研判，目的是有效的安全决策和响应。

**预测、预防：**建立风险通报和威胁预警机制，全面掌握攻击者目的、技战术、攻击工具等信息。

**防御：**利用掌握的攻击者相关目的、技战术、攻击工具等情报，完善防御体系。

数据库审计系统

根据信息安全等级保护基本要求：审计范围应覆盖到服务器和重要客户端上的每个操作系统用户和数据库用户。

建议部署1台数据库审计系统，用作当前数据库审计应用。时刻了解数据库的使用状况，对数据库的操作及数据库调用进行审计分析，并在出现问题时能及时的发现问题所在，以便解决问题，避免和挽回不必要的损失。

* **基本参数**

|  |  |  |
| --- | --- | --- |
| 产品类型 | 数据库审计系统 | |
| 接入模式 | 旁路 | |
| 部署位置 | 部署在核心区域或服务器区 | |
| 主要功能 | 数据库审计 | 1、支持Sybase、DB2、SQLServer、Oracle、MYSQL、Informix、PostgreSQL达梦、南大通用Gbase、人大金仓等多种主流数据库监控与审计，通过应用协议自动识别技术，结合灵活的审计策略，实现对数据库的完整审计  2、支持SQL操作回放 |
| 细粒度审计规则 | 1、审计的内容：SQL 语句、SQL 语句参数、执行结果（成功、失败和详细的失败原因）、被影响的记录、详细的查询结果集、事务状态、会话登录和登出信息等  2、审计的范围：对象、操作、SQL 分类类型、用户、指定的客户端（IP、MAC）、客户端工具或应用系统等  3、提供实时的数据库审计、风险评估引擎、漏洞攻击监测引擎、细粒度访问监测引擎的告警数据 |
| 双向审计 | 提供对双向数据包的解析、识别，不仅能够识别用户的请求，还能够对数据库的应答做了详细的统计，包括命令执行的时长、影响行数、应答码等信息 |
| 应用用户关联审计 | 可以追溯到应用层的原始访问者及请求信息（如：操作发生的 URL、客户端的 IP 等信息） |
| 报表分析与可视化展示 | 提供专业化的报表和分析图表，统计结果支持柱状图、饼图、曲线图与负载图展示 |
| 管理配置 | 数据备份和还原 | 对 SQL 日志、运行期数据和策略中心的数据进行自动备份、手动备份、备份还原以及数据自动清理功能 |
| 告警响应 | 支持手机短信、邮件报警、屏幕、Syslog、SNMPTrap、声音报警、执行脚本（联动）等多种报警方式 |

综合日志管理系统

根据《网络安全法》第二十一条“采取监测、记录网络运行状态、网络安全事件的技术措施，并按照规定留存相关的网络日志不少于六个月”。

同时根据《信息安全等级保护基本要求》：应对系统中的网络设备、主机、应用运行状况、网络流量、用户行为等进行日志记录；审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；应能够根据记录数据进行分析，并生成审计报表；应对审计记录进行保护，避免受到未预期的删除、修改或覆盖等。

建议部署一台综合日志审计系统，通过集中采集网络设备、安全设备、主机等日志的安全事件、用户访问记录、系统运行日志、系统运行状态、网络存取日志等各类信息，经过规范化、过滤、归并和告警分析等处理后，以统一格式的日志形式进行集中存储和管理。

* **基本参数**

|  |  |  |
| --- | --- | --- |
| 产品类型 | 综合日志审计系统 | |
| 接入模式 | 旁路 | |
| 主要功能 | 数据采集 | 支持通过页面直接将日志文件导入或以syslog方式接收日志信息，支持日志类型：UNIX、WINDOWS事件[2000、2003、2008、XP、VISTA、Win7及以上版本]、网络及安全设备、AS400日志、数据库访问[Mysql]、WEB访问[Apache、IIS、Tomcat、Nginx、Weblogic、Resin、Websphere]、文件访问[VSftpd、Pureftpd、NCftpd、IISftpd、Proftpd、Glftpd、Serv-u]、数据库服务[Oracle、Mssql、Mysql、DB2、Informix、Sybase]、WEB服务[Apache、Tomcat、Nginx、Weblogic、Resin、Websphere]、FTP服务[VSftpd、NCftpd、Proftpd、Glftpd、Serv-u] |
| 支持SNMP日志采集，支持日志类型：网络及安全设备[至少单位产品品牌] |
| 支持镜像数据采集，支持类型：数据库模块[Oracle、Mssql、Mysql、DB2、Informix、Sybase]、文件传输模块[FTP、SMB、HTTP]、邮件模块[SMTP、POP、HTTP]、即时通讯模块[淘宝旺旺、MSN、QQ]、远程控制模块[Telnet]、网站访问模块[网页浏览、论坛微博]、入侵检测、业务检测、流量监控 |
| 监控功能 | 支持以图表方式（饼图、柱图、曲线图）显示当日日志数据分布情况 |
| 支持自定义配置实时监控的日志类型 |
| 支持对所添加的资产进行实时监控，并能以不同图标显示发生的事件及告警 |
| 支持以图表方式（饼图、柱图、曲线图、清单列表）显示当日安全事件及告警日志数据分布情况 |
| 支持实时监控本系统当前运行状态，包括系统CPU、内存、硬盘状态及管理员操作 |
| 数据管理功能 | 支持按日志属性、日志类型、时间范围等进行数据备份 |
| 支持WEB界面备份及日志恢复导入工作 |
| 支持自动与手动两种备份归档方式 |
| 系统支持以FTP上传方式将归档文件存储到第三方存储系统中 |
| 管理配置 | 系统管理 | 1、B/S方式，采用HTTPS方式远程安全管理，无需安装管理客户端 2、无需另外安装软件组件，即可通过 SNMP Trap、Syslog、ODBC\JDBC、文件\文件夹、WMI、FTP、NetBIOS、OPSEC等多种方式完成日志收集功能 3、支持管理员权限分级 4、支持对管理员登录IP地址的限制 5、支持身份鉴别安全策略，支持但不限于如密码长度、复杂度、密码历史、登录失败限制、有效期等策略控制 |
| 日志报警 | 1、审计日志文件方式存储 2、审计日志加密导出审计系统 3、支持对所有审计管理员操作审计系统的动作进行审计 4、显示日志内容包括：接收时间、事件类型、事件名称、报警级别、来源IP、目的IP、设备类型、设备来源IP等 |
| 报表分析功能 | 1、系统内置多种类报表模板 2、支持动态\静态（日报、周报、月报）两种系统生成方式 3、支持报告的邮件转发、生成提醒功能；支持多人邮件接收 4、支持自定义审计报告 5.、支持导出html、Excel、PDF |
| 查询分析功能 | 1. 支持多种方式的查询检索，包括：日志检索、事件检索、告警检索、高级检索及文件检索；  2. 支持以日志类型、时间范围及条件字段快速检索过滤； 3. 支持高级检索以多条件组合查询方式，可以将每一个日志字段作为查询条件进行查询； 4. 支持按日志文件的名称、内容进行检索，并提供页面下载原始日志文件； 5. 支持查询模版创建、修改、删除功能； 6. 支持查询结果导出； |
| 资质需求 | 公安许可需求 | 具备公安部颁发的《计算机信息系统安全专用产品销售许可证》 |

主机安全防护

主机集中病毒防护软件

根据信息安全等级保护基本要求：应安装防恶意代码软件，并及时更新防恶意代码软件版本和恶意代码库；应支持防恶意代码的统一管理。

建议部署1套防恶意代码杀毒软件，部署在各服务器和终端。构建了统一的防病毒集中管理，保证整个防毒产品可以从病毒监控管理中心及时得到更新，同时又使系统管理人员可以在任何时间通过管理控制台对整个防毒系统进行集中管理，使整个系统中任何一个节点都可以被管理人员随时管理，保证整个防毒系统有效、及时地拦截病毒。

* **基本参数**

|  |  |  |
| --- | --- | --- |
| 产品类型 | 集中病毒防护（软件） | |
| 接入模式 | 终端 （需安装客户端） | |
| 部署位置 | 至少部署在windows环境下的主机 | |
| 主要功能 | 产品支持 | 支持 Netware, Windows NT/2000/2003/2008 Server、x86\_64位CPU 、支持Red Hat Enterprise Linux 4.0 (AS, ES, WS, Desktop) (i686 and x86\_64)、Red Hat Enterprise Linux 5 (Server or Desktop) (i686 and x86\_64) 、SUSE(TM) Linux Enterprise 10/11 (Server or Desktop) (i686 and x86\_64)、CentOS 4/5、NetApp存储服务器、EMC存储服务器等系统。 |
| 系统功能 | 1、具备病毒爆发防御功能。当最新病毒爆发时，可在病毒代码未完成之前自动对网络中的病毒传播端口、共享等进行关闭，切断病毒传播途径，预防最新病毒的攻击。 2、支持云安全扫描和传统病毒码扫描两种运行方式。 3、支持与微软AD的集成，可套用AD的分组方式，方便管理（可选） 4、支持对USB、软驱、光驱、网络共享的使用权限进行控制。 5、具备个人防火墙功能，可对多种协议数据包进行阻挡，可对网络中异常浏览进行监控。  6、不需要人工辅助，客户端集成“病毒专杀”工具，“病毒专杀”工具必须支持目前最流行的新型态病毒。  7、管理控制台可以直接控制实现客户端恢复动作。 8、可赋予客户端对“预设扫描”的控制权限，比如延迟扫描、跳过扫描、停止扫描等（可选） 9、具备远程病毒集中清除功能。可对网络中感染病毒的计算机进行远程自动清除，无需知道计算机的物理位置，无需到客户端逐一清除病毒。 10、对于蠕虫、特洛伊木马等恶意程序的专杀工具能够随产品在线自动更新，无需手动下载。 11、采用智能型扫描机制，能够以文件真正格式作扫描，通过文件头的真实信息而不是简单的通过文件扩展名来识别文件的类型，以提高扫描效率。 12、病毒处理方式必须支持智能式的处理方式。根据不同的病毒类型，采取不同的处理策略。 13、防病毒产品必须要支持网络病毒识别码，网络病毒识别码与传统的病毒代码不同，网络病毒识别码能够识别网络病毒攻击行为。在客户端实现网络病毒的封包过滤。 14、具备病毒源准确定位功能，快速查获病毒。 15、可对客户端进行逻辑分组，对不同的客户端实行不同的防毒管理策略。 |
| 管理配置 | 易管理性要求 | 1、管理端病毒代码及引擎升级可通过多种方式，如通过升级工具直接升级以满足大多内网用户升级的需要 2、防病毒管理必须提供Web管理方式；管理通讯采取加密措施。 |
| 安装部署 | 1、客户端软件提供多种方式的分发、安装方法。必须支持WEB安装方式、SMS安装方式、MSI程序打包安装方式、共享安装等。 2、产品安装、卸载、代码或引擎升级均无需重新启动操作系统。 3、客户端产品防毒服务关闭和产品卸载均需提供密码保护功能，预防防毒系统漏洞的出现（可选） |
| 资质需求 | 公安许可需求 | 具备公安部颁发的《计算机信息系统安全专用产品销售许可证》 |

应用安全防护

Web应用防火墙系统

根据信息安全等级保护基本要求：应对Web部署应用防火墙设备，启用Web防护、DDOS防护、网页防篡改等相关功能。

建议将WAF串行部署在WEB服务器前端，用于检测并阻断异常流量，构建统一Web及IP安全防护。

* **基本参数**

|  |  |
| --- | --- |
| **硬件规格** | **产品参数** |
| 产品类型 | Web应用防火墙 |
| 部署方式 | 镜像监测模式、镜像阻断模式、透明代理模式、透明检测模式、反向代理模式、路由模式、DNAT转化模式、网关模式 |
| 串行配置管理接口（个） | 1 |
| USB接口（个） | 2 |
| 千兆电口 | 板载6 个100/1000M 电口 |
| BYPASS（组） | 2 |
| 硬盘（G） | 1T |
| 可扩展情况 | 自带一个扩展槽 |
| 机箱 | 2U 机架式设备 |
| 电源 | 冗余双电源 |
| 性能指标 | |
| HTTP吞吐量（Gbps） | 3.5Gbps |
| HTTP新建连接数（CPS） | 12,000/s |
| HTTP新建事务数（TPS） | 28,000/s |
| HTTP 最大并发连接数 | 2,000,000 |
| DDoS清洗能力（Mpps） | 1.52Mpps |
| 产品资质 | |
| 基本要求 | 资质参数 |
| 产品资质 | 具有中华人民共和国公安部的《计算机信息系统安全专用产品销售许可证》 |
| 具有Web防护产品软件著作权 |
| 具有OWASP Web防火墙基准测试证书 |
| 类别 | 具体技术指标及参数要求 |
| 硬件指标 | 系统应为机架式独立硬件设备，全内置封闭式结构，具有完全自主知识产权的专用安全操作系统，稳定可靠 |
| 镜像阻断 | ★支持旁路镜像部署模式下，对检测到的攻击进行旁路阻断（要求提供配置截图） |
| 网络安全 | 支持ARP绑定 |
| 支持策略路由管理 |
| 提供DNS服务器功能，支持服务器泛域名和普通域名服务（要求提供配置截图） |
| 支持DNAT/SNAT |
| 支持静态及动态黑白名单策略 |
| 支持基于源目的IP、端口服务和时间等元组的包过滤功能 |
| Web安全防御 | 支持HTTP协议校验，可根据实际网络状况自定义协议合规标准，过滤非法数据 |
| 支持HTTP访问控制，可根据实际网络状况自定义请求方法等参数的访问控制规则，过滤非法请求 |
| 支持HTTPS防护 |
| 应能识别和阻断注入攻击 |
| 支持防扫描陷阱（要求提供配置截图） |
| 支持爬虫防护（要求提供配置截图） |
| 支持文件上传、下载过滤（要求提供配置截图） |
| 支持LDAP、XPATH、struct2/xworks检测和防护 |
| 应能识别阻断跨站脚本(XSS)注入式攻击 |
| 应能识别阻断盗链攻击 |
| 应能识别阻断跨站请求伪造攻击 |
| 非法上传检测阻断，包括恶意WebShell防护 |
| 对网页请求/响应内容中的非法关键字进行检测、过滤 |
| 应能识别和防止敏感信息泄露 |
| 支持弱密码保护功能 |
| 支持恶意代码攻击、错误配置攻击、隐藏字段攻击、会话劫持攻击、参数篡改攻击、缓冲区溢出攻击防护 |
| 提供多种威胁处理方式：返回错误码、重定向、日志监控、封禁等 |
| 安全部署 | ★支持网站自学习（要求提供配置截图） |
| 支持自动封禁策略，自动屏蔽网站的异常攻击（要求提供配置截图） |
| 支持自定义防护策略，提供初级、中级、高级的初始防护策略模板（要求提供配置截图） |
| 一键断网 | 支持通过移动终端管理，实现网站快速应急处置； |
| ★支持网站批量离线、网站批量恢复、网站一键断网、网站一键恢复操作（要求提供配置截图） |
| 虚拟环境支持 | 支持部署在Vmware、KVM等虚拟环境 |
| 支持IDE、virtio等虚拟磁盘模式 |
| 威胁情报支持 | ★支持第三方威胁情报库更新 |
| ★支持利用威胁情报规则进行防护，并支持基于威胁情报的日志查询（提供配置界面及日志截图） |
| 云防护支持 | ★支持与云清洗中心进行实时联动，并提供配置界面和流量统计图表（提供配置界面及图表截图） |
| ★支持云Web攻击清洗与云CC攻击清洗（要求提供配置截图） |
| 网页防篡改 | 能进行配置自动分发功能（要求提供配置截图） |
| 应采用内核级防篡改保护，能及时阻止并报告攻击事件； |
| 应至少同时支持Windows、Linux、IBM Unix操作系统的的网页防篡改； |
| 应支持支持超过40GB以上网页防篡改保护和恢复功能 |
| ★应能支持对所有安装防篡改客户端的服务器进行集中管理（要求提供配置截图） |
| 能监控所有服务器状态、防篡改信息 |
| 监控响应时间 小于0.5秒 |
| 篡改恢复时间 小于0.1秒 |
| 资源占用 在对比网页篡改防护系统未运行时的增长须小于20% |
| 业务响应 在对比网页篡改防护系统未运行时的增长须小于20% |
| 支持IIS、Weblogic、Websphere、Apache、Tomcat等 |
| 网页防篡改同步 | 系统可以从本地或异地备份文件夹自动同步到监测目录中 |
| 系统支持增量备份功能。 |
| 系统支持各种发布工具或发布方式。 |
| 系统支持主/备目录和主/备服务器两种备份模式 |
| 支持防篡改中心和发布中心的负载均衡部署模式（要求提供配置截图） |
| DDoS支持 | ★要求必须具备独立的网络层DDoS防护模板和应用层DDoS防护模板（要求提供配置截图） |
| ★要求必须不能依赖对包数做阈值的简单限制来实现DDoS防护，至少具备以下处理方法：源路由限制；分片报文限制、分片报文和重组报文长度的独立配置；ping包限制、ping包长度配置；ICMP长度配置、单个ICMP报文速率配置和单个ICMP字节速率的独立配置；ACK扫描、SYN/ACK扫描、RST扫描、FIN扫描的独立配置；总扫描速率与单个IP扫描速率的独立配置（要求提供配置截图） |
| ★要求CC攻击防护必须支持真实浏览器验证功能，同时支持对IP失败速率的验证配置（要求提供配置截图） |
| ★提供动态基线模式，能对所有流量进行动态建模，减少误报，更精细进行控制 |
| ★要求支持云端与设备端联动，实现CC攻击云防护（要求提供配置截图） |
| 审计功能及告警 | 要求至少具备独立的审计日志、流量日志、攻击日志、网页防篡改日志、DDoS防护日志及威胁情报日志模块，且日志支持syslog方式外发（要求提供配置截图） |
| 支持日志自动备份（要求提供配置截图） |
| ★要求攻击日志具备详细的攻击摘要和原始报文（要求提供配置截图） |
| ★要求攻击日志具备一键关联白名单排除策略（要求提供配置截图） |
| 要求至少支持日志、trap、邮件、短信等告警方式（要求提供配置截图） |
| 统计及报表 | 系统须能够对遭受攻击按照攻击次数、防护的网站、遭受攻击的网页、攻击类型、攻击时间（或者发现攻击的时间）等进行统计并排名 |
| 能够根据网站的访问防护的网站、被篡改内容、篡改内容的类型、试图进行的篡改、成功的篡改、发现的日期、事件发生的日期等条件进行详细信息的查询 |
| 支持以Word、PDF、HTML等通用格式导出报表 |
| 升级系统 | 支持系统离线升级 |
| 支持规则库离线升级和在线升级 |
| 支持每月至少提供一次规则升级；紧急事件24小时内提供升级 |
| Web漏洞扫描 | 提供Web站点安全扫描功能 |
| 支持自定义Web安全扫描任务，定期进行Web安全扫描 |
| SNMP | 支持SNMP V1 V2 V3 |
| 支持SNMP trap |
| 集中管理 | 能够通过集中管理平台进行状态集中监控、配置集中管理、日志集中分析 |
| 能实时检测各WAF工作状态以及系统关键资源的运行状态 |
| 管理界面 | 支持HTTPS、SSH、Console、WebShell多种管理方式 |
| 支持Web管理端口自定义 |
| 备份恢复 | 支持系统配置的手工备份、自动备份（自动备份以日、周、月区分） |
| 支持备份配置导入、导出； |
| 系统诊断 | 支持界面生成远程技术支持文件，可直接从界面生成并提取； |
| 支持在线抓包功能 |
| 支持界面诊断工具，可直接通过web界面进入cli管理通道（要求提供配置截图） |
| BYPASS | 支持硬件bypass功能； |
| 支持软件bypass负载保护机制，设备达到峰值时，切换bypass功能 |
| 高可用性 | 支持向导配置（要求提供配置截图） |
| 支持VRRP协议 |
| 支持主-主、主-备双机模式 |
| 支持配置同步 |
| 易用性 | 管理系统支持中英文二种版本 |

数据安全防护

数据防泄露系统

根据信息安全等级保护基本要求，网络设备、操作系统、数据库系统和应用系统的鉴别信息、敏感的系统管理数据和敏感的用户数据应采用加密或其他有效措施实现传输保密性；当使用便携式和移动式设备时，应加密或者采用可移动磁盘存储敏感信息；用于特定业务通信的通信信道应符合相关的国家规定。

根据企业实际需求，可采用网关方式或B/S部署方式安装数据防泄露设备，用于企业文件外发管理、数据主动备份、电子文件管理、打印安全管理、桌面安全管理等保证数据安全。

* **基本参数**

|  |  |  |
| --- | --- | --- |
| 产品类型 | 数据防泄露系统 | |
| 接入模式 | 串行或B/S方式 | |
| 部署位置 | 部署在出口网关或其它安全运营区域 | |
| 主要功能 | 内容安全保护 | 拷贝拖拽控制  插入链接控制  另存为控制  截屏控制(控制范围)  动态屏幕水印保护  加密文件打印控制  打印控制区分真实打印与虚拟打印  动态打印水印保护  Office剪贴板控制  打印盲水印  防病毒木马窃取数据 |
| 数据隔离防护 | 支持强制隔离控制  智能隔离密钥管理(非手动管理)  支持特权用户(跨隔离范围访问)  隔离文件权限(只读打印等)  支持按业务隔离(数据类型) |
| 应用系统防护 | 保护所有类型应用系统(C/S(含插件)、B/S)  支持指定类型下载加密  支持指定类型上传解密  应用系统明文保护  应用系统防伪冒  与应用系统深度结合(第三方开发接口) |
| 文档外发 | 文件支持打包方式带出及使用  支持exe格式外发包（免手动安装阅读器)  非exe格式外发包(防杀软拦截)  支持多文件多目录同时外发  支持关联文件外发  支持exe可执行文件的外发  外发包无大小限制  外发包使用环境支持win7x64、win 8.1 X64  外发包使用环境无windows用户权限限制  外发包权限支持USBKey控制  外发包内文件支持主动删除  外发包文件禁止导出控制(驱动层) |
| 权限管理 | 防另存为等脱密控制（驱动层）  以文件为主体的控制方式(无需配置进程策略） |
| 管理配置 | 审批流程 | 支持多级审批  支持不同部门配置不同审批流程  支持审批过程的自动通知(邮件/消息) |
| 策略配置 | 支持自定义策略配置  多用户策略支持  进程签名策略 |
| 其它 | 邮件附件控制 | 邮件附件审批解密  邮件附件发送自动解密(所有类型/指定类型)  邮件附件显示加密图标 |
| 其他安全防护/性能及稳定性参数 | 钩子防摘除  防内存转储  防进程伪造/欺骗  防远程线程注入  防OLE调用  未支持第三方文件系统另存泄密  office宏导出控制 |
| 加解密方式 | 进程(文件级)加密  磁盘级加密  驱动层透明加密(无明文临时文件)  驱动层半透明加密(无明文临时文件)  基于Minifilter框架  兼容网络文件系统  兼容第三方文件系统  支持Windows系统(32位/64位,win8)  支持Linux系统  支持移动终端(Ios/Android)  支持虚拟化环境(Citrix/Vmware) |

## 整改信息安全服务规划

### 定级备案协助

根据《信息安全等级保护管理办法》，信息系统安全保护等级为第二级以上的信息系统运营使用单位或主管部门，应当在安全保护等级确定后，到当地公安机关网监部门办理备案手续。根据XXXXXXXXXX的实际情况，因此需要完成安全保护等级备案工作。

* **信息系统定级原则**

信息系统作为保护对象，《管理办法》中将信息系统分为五级，分别为：

第一级，信息系统受到破坏后，会对公民、法人和其他组织的合法权益造成损害，但不损害国家安全、社会秩序和公共利益。

第二级，信息系统受到破坏后，会对公民、法人和其他组织的合法权益产生严重损害，或者对社会秩序和公共利益造成损害，但不损害国家安全。

第三级，信息系统受到破坏后，会对社会秩序和公共利益造成严重损害，或者对国家安全造成损害。

第四级，信息系统受到破坏后，会对社会秩序和公共利益造成特别严重损害，或者对国家安全造成严重损害。

第五级，信息系统受到破坏后，会对国家安全造成特别严重损害。

* **信息系统业务安全性分析**

通过对信息系统所承载业务及业务流程的分析，分析信息系统内信息资产和信息系统所提供服务的重要性，协助用户判断信息系统中业务信息和所提供的服务机密性、完整性或可用性等安全属性遭到破坏后，对国家安全利益、经济建设、公共利益或单位利益所造成的影响程度。为子系统划分和信息系统定级打下扎实基础。

* **系统划分**

对于承载多项业务的用户信息系统，我院在深入分析各项业务性质、特点及信息系统的实际情况基础上，对信息系统按业务子系统进行合理划分。

* **系统辅助定级**

依据《信息系统安全保护等级定级指南》所提出的4个定级要素，灵活运用指南中所提出的确定信息系统安全保护等级的步骤和方法，在信息系统业务安全性分析的基础上，提出等级建议，协助用户进行系统定级。

* **协助用户完成等级备案**

根据公安部等级保护相关备案要求，协助客户完成等级保护备案工作，编写定级报告和备案表，获得信息系统安全等级保护备案证明。

### 安全差距评估

评估目标

依据《信息系统安全等级保护基本要求》、《信息系统安全等级保护测评要求》，对XXXXXXXXXX信息系统备案安全等级相对应的测评项进行符合性测评，检查、分析XXXXXXXXXX信息系统的安全现状与所备案安全等级要求之间的差距，了解单位信息系统的现状，确定不符合安全项。并出具是否满足信息系统安全保护等级的差距评估报告，用以指导信息系统等级保护安全整改工作。

差距评估流程

1. 确定评估方案

我院对信息系统开展前期调研，根据定级报告中被评估信息系统的安全等级（S，A，G），从等级保护基本要求的指标中选择和组合评估用的安全指标，形成一套信息系统的评估指标，作为差距分析评估的依据；将具体差距分析评估对象和评估指标进行结合，确定评估范围，形成评估使用的评估方案。

1. 准备差距分析表

我院通过准备好的差距分析表，与客户确认现场沟通的对象（部门和人员），准备相应的检查内容。

 差距分析表包含以下内容：

* 安全技术差距分析：包括网络安全、主机安全、应用安全、数据安全及备份恢复；
* 安全管理差距分析：包括安全管理制度、安全管理机构、人员安全管理、系统建设管理；
* 系统运维差距分析：包括环境管理、资产管理、介质管理、监控管理和安全管理中心、网络安全管理、系统安全管理、恶意代码防范管理、密码管理、变更管理、备份与恢复管理、安全事件处置；
* 物理安全差距分析：包括物理位置的选择、物理访问控制、防盗窃和防破坏、防雷击、防火、防水和防潮、防静电、温湿度控制、电力供应、电磁防护。
* 不同安全保护级别的系统所使用的差距分析表的内容也不同。

1. 现场差距分析

我院根据所确定的安全评估指标和安全评估方案，通过询问、检查和测试等多种手段，将系统现状与安全评估指标进行逐一对比，记录当前的现状情况，找到与评估指标之间的差距。

**判断安全管理方面与评估指标的符合程度**

通过观察现场、询问人员、查询资料、检查记录等方式进行安全管理方面的评估，准确记录评估结果，判断安全管理的各个方面与评估指标的符合程度，给出判断结论。

**判断安全技术方面与评估指标的符合程度**

通过观察现场、询问人员、查询资料、检查记录、检查配置、技术测试、渗透攻击等方式进行安全技术方面的评估，准确记录评估结果，判断安全技术的各个方面与评估指标的符合程度，给出判断结论。

1. 生成差距分析报告

完成现场差距分析之后，我院项目组归纳整理、根据等级指标对比评估结果记录，结合被评估单位提供的各种资料，进行全面的综合分析，找出目前信息系统与等级保护安全要求之间的差距，明确不符合项，生成《安全差距分析报告》。

差距评估内容

1. 安全技术评估

* **物理环境安全评估**

主要考察信息系统所在物理环境（包括中心机房和各处配线间）相关的防火、防水、防雷、防盗和不间断电源等保障物理安全的各种设施。

* **计算机网络安全评估**

检查、测试网络拓扑结构、城域网和互联网连接的路由器、交换机、防火墙以及其他信息安全设备、各应用服务器的基本配置和安全策略；检查整体网络的数据流信息。

* **操作系统安全评估**

检查、测试所有网络设备、信息安全设备和服务器的操作系统，检查所有设备的windows、Linux和专业操作系统的基本配置和安全策略。是否及时安装最新补丁进行针对性检查。

* **应用系统安全评估**

对所有业务系统和门户网站等重要信息系统进行安全配置检查和测试。

* **数据库安全评估**

对各种数据库进行安全检查和测试。例如某业务系统中数据库是否安装最新补丁，管理帐户是否存在弱口令等进行检测。

* **未控制网络链接评估**

获得所有未控制并能够连接到网络的设备信息（例如调制解调器、第二块网卡、USB网卡、1394接口网卡等）。防止未经授权的拨入。

* **防病毒及恶意软件评估**

检查所有服务器的杀毒软件系统和单机防恶意软件系统

* **灾难恢复策略评估**

审核并检查数据备份及灾难恢复计划，了解是否进行应急演练，并提出改进建议 。

* **安全控制策略评估**

边界访问控制的防火墙、入侵检测、防病毒等设备的配置策略。负责安全政策的编制管理人员、办公人员的安全意识、各种安全管理规章制度等。

1. 安全管理评估

通过查阅文档、抽样调查等方法，针对被测单位在信息安全方面制定规章制度的合理性、适用性等进行评估，主要包括安全管理机构、安全管理制度、人员安全管理、系统建设管理和系统运维管理等内容。

**人员访谈**

内容：针对组织内的安全管理人员、安全员、安全主管、工作人员、关键活动批准人、管理人员、机房值守人员、人事负责人、人事工作人员、审计员、网络管理员、文档管理员、物理安全负责人、系统管理员、系统建设负责人、系统运维负责人、资产管理员等不同类型岗位的人员访谈

**文档检查**

内容：安全管理机构、安全管理制度、人员安全管理、系统建设管理、系统运维管理等方面的文档检查。

### 安全整改设计

信息安全整改建议在其安全差距评估所发现的安全隐患和问题的基础上，按照国家等级保护相关建设规范和技术要求，结合被评估单位的信息系统的真实情况和具体需求，设计完善、全面、合规的整改方案，保证XXXXXXXXXX信息系统在按照整改方案进行合规性整改后，可控制安全隐患和问题，同时安全防护能力达到《信息安全技术信息系统安全等级保护基本要求》中相关技术和管理要求。

人工安全策略加固

根据安全整改建议和安全评估报告所列出的安全配置、策略的不符合项，逐一进行加固，主要针对硬件设备（如交换机、路由器、防火墙等）、不同的操作系统（如Windows、UNIX、INUX、Soaris等）、不同的应用（如Web服务、FTP服务、E-mai服务、数据库应用等）进行安全加固。加固完成后，使其相关硬件和软件达到等保合规性要求。安全加固流程如下：

* **资产调研**

收集需要进行安全加固的信息系统所涉及的主机、数据库及中间件资产的信息情况，填写《信息资产调查表》，完成信息资产的信息收集。确定需要加固的设施范围。

* **加固方案编写**

对加固范围内的主机操作系统、网络设备、数据库系统及应用中间件系统进行评估，检查这些系统目前安全状况，根据现状制定相应的安全加固措施，形成安全加固计划，对《安全加固实施计划》进行讨论，确定计划。

* **现场加固**

根据制定的加固计划，安全加固操作主要针对主机操作系统、网络设备、数据库系统及应用中间件系统进行加固，比如正确的安装软硬件、安装最新的操作系统和应用软件的安全补丁、操作系统和应用软件的安全配置、系统安全风险防范、系统安全风险测试、系统完整性备份、系统账户口令加固等等。并对加固后的系统进行全面的测试，确保加固对系统业务无影响，并达到了安全提升的目的。

* **编写加固报告**

根据安全加固实施记录，提交最后的《安全加固报告》。记录了加固的完整过程和有关系统安全管理方面的建议或解决方案。

管理制度建设与优化

根据安全整改建议和安全评估报告所列出的管理制度相关问题，对于缺少的管理制度进行完善，对已有的管理制度进行优化。最终编写一套符合等级保护标准要求的安全管理制度集。主要从如下内容考虑：

* **安全管理机构**

加强和完善安全机构的建设，设立指导和管理信息安全工作的信息安全领导小组，设立安全主管、安全管理各个方面的负责人，明确定义各个工作岗位的职责。建立各种安全管理活动的审批程序，明确对内对外的沟通协作方式，建立对各项安全管理活动的监督审核机制。

* **安全管理制度**

在安全评估的基础上，建立信息安全工作总体方针、安全策略，以方针策略为依据建立配套的安全管理制度及流程规范，由专门的组织机构负责管理制度的制订、发布和贯彻落实。定期对制度进行评审和修订，确保安全管理制度的适用性。

* **人员安全管理**

主要涉及两方面，对内部人员的安全管理和对外部人员的安全管理。具体包括人员录用、人员离岗、人员考核、安全意识教育和培训和外部人员访问管理等方面。

* **系统建设管理**

建设符合安全等级保护要求的信息系统、系统建设管理主要关注的是信息系统生命周期中的前三个阶段（即设计、采购、实施）中各项安全管理活动，实现信息系统的安全管理贯穿系统的整个生命周期。系统建设管理分别从工程实施建设前、建设过程以及建设完毕交付等三方面考虑，具体包括系统定级、安全方案设计、产品采购和使用、自行软件开发、外包软件开发、工程实施、测试验收、系统交付、系统备案、等级测评和安全服务商选择等方面。

* **系统运维管理**

系统运行涉及到很多管理方面，要保证系统始终处于相应安全保护等级的安全状态中。要监控系统发生的重大变化，以便修改对应的安全措施。系统运维管理主要包括环境管理、资产管理、介质管理、设备管理、监控管理和安全管理中心、网络安全管理、系统安全管理、恶意代码防范管理、密码管理、变更管理、备份与恢复管理、安全事件处置、应急预案管理等方面。

### 等级保护验收测评

对信息系统进行等级保护测评是等级保护制度的一个重要环节，也是对信息系统进行安全建设和管理的重要组成部分。根据前期对信息系统的安全整改情况，进行最终的验收测评，并提交符合国家信息安全等级保护主管部门要求的验收测评报告。

#### 测评流程

1. 测评准备阶段
   * 测评项目组组建：明确项目经理、测评人员及职责分工。
   * 项目计划书编制：项目计划书包含项目概述、工作依据、技术思路、工作内容和项目组织等。
   * 信息系统调研：通过查阅被测系统已有资料或使用调查表格的方式，了解整个系统的构成和保护情况，明确被测系统的范围（特别是信息系统的边界），了解被测系统的详细构成，包括网络拓扑、业务应用、业务流程、设备信息（服务器、数据库、网络设备、安全设备、数据库等）、管理制度等。
   * 工具和表单准备：根据被测系统的实际情况，准备测评工具和各类测评表单。
2. 方案编制阶段
   * 测评对象确定：根据已经了解到的被测系统信息，分析整个被测系统及其涉及的业务应用系统，确定出本次测评的测评对象。
   * 测评指标确定：根据已经了解到的被测系统定级结果，确定出本次测评的测评指标。
   * 测评工具接入点确定：确定需要进行工具测试的测评对象，选择测试路径，根据测试路径确定测试工具的接入点。
   * 测评内容确定：确定现场测评的具体实施内容，即单元测评内容。
   * 测评实施手册开发：编制测评实施手册，详细描述现场测评的工具、方法和操作步骤等，具体指导测评人员如何进行测评活动。
3. 现场测评阶段

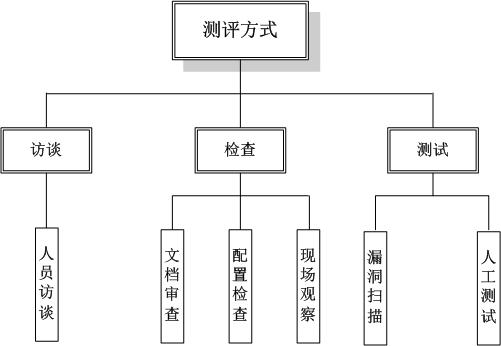
现场测评分别从技术上的物理安全、网络安全、主机系统安全、应用安全和数据安全五个层面和管理上的安全管理机构、安全管理制度、人员安全管理、系统建设管理和系统运维管理五个方面分别进行。

* 现场测评的访谈、检查、测试工作需要进入信息系统所在机房，与XXXXXXXXXX工作人员进行座谈，使用工具对XXXXXXXXXX网络、设备等进行现场检查和测试，因此，需要XXXXXXXXXX安排相应的时间、地点、人员配合测评工作；
* 在测评过程中测评机构可能需要用到XXXXXXXXXX相关数据和资料（如：机房设计文档、网络拓扑图、网站系统测试帐号、网站系统建设资料、系统日志等），XXXXXXXXXX需要尽力配合提供；
* XXXXXXXXXX应安排相关人员提供现有的管理制度集，XXXXXXXXXX应就制度中部分具体事项（如具体人员、机构、流程等）应给予明确回复以确保管理制度集符合XXXXXXXXXX的实际情况。

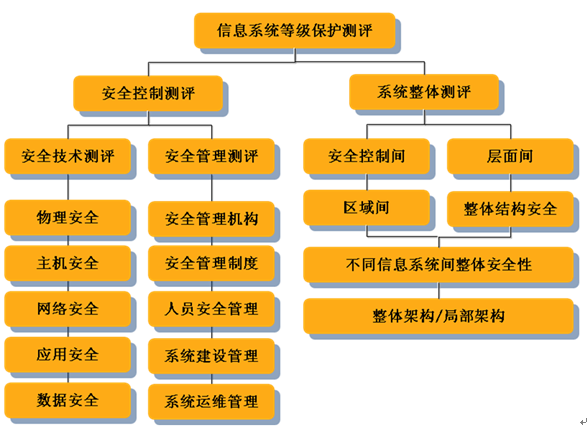
1. 分析与报告编制阶段
   * 单项测评结果分析：针对测评指标中的单个测评项，结合具体测评对象，客观、准确地分析测评证据。
   * 单元测评结果判定：将单项测评结果进行汇总，分别统计不同测评对象的单项测评结果，从而判定单元测评结果，并以表格的形式逐一列出。
   * 整体测评：针对单项测评结果的不符合项，采取逐条判定的方法，从安全控制间、层面间和区域间出发考虑，给出整体测评的具体结果，并对系统结构进行整体安全测评。
   * 风险分析：据等级保护的相关规范和标准，采用风险分析的方法分析等级测评结果中存在的安全问题可能对被测系统安全造成的影响。
   * 等级测评结论形成：在测评结果汇总的基础上，找出系统保护现状与等级保护基本要求之间的差距，并形成等级测评结论。
   * 测评报告编制：根据等级测评结论，编制测评报告，包括概述、被测系统描述、测评对象说明、测评指标说明、测评内容和方法说明、单元测评、整体测评、测评结果汇总、风险分析和评价、等级测评结论等。

测评方式

依照《信息安全技术信息系统安全等级保护测评要求》（国标报批稿）的要求，在本次信息系统安全等级保护测评过程中，我院所采用的现场测评方法主要包括访谈、检查和测试。



测评内容



1. **安全技术测评**

物理安全：测评信息系统的物理安全保障情况。主要涉及对象为物理基础设施。在内容上，物理安全层面测评实施过程涉及10个测评单元，包括：物理位置的选择、物理访问控制、防盗窃和防破坏、防雷击、防火、防水和防潮、防静电、温湿度控制、电力供应、电磁防护。

网络安全：测评信息系统的网络安全保障情况。主要涉及对象为网络互联设备、网络安全设备和网络拓扑结构。在内容上，网络安全层面测评实施过程涉及7个测评单元，包括：结构安全、访问控制、安全审计、边界完整性检查、入侵防范、网络设备防护、恶意代码防范。

主机安全：测评信息系统的主机安全保障情况。主要涉及对象为各类服务器的操作系统、数据库管理系统。在内容上，主机系统安全层面测评实施过程涉及7个测评单元，包括：身份鉴别、访问控制、安全审计、入侵防范、恶意代码防范、资源控制、剩余信息保护。

应用安全：测评信息系统的应用安全保障情况，主要涉及对象为各类应用系统。在内容上，应用安全层面测评实施过程涉及9个测评单元，包括：身份鉴别、访问控制、安全审计、通信完整性、通信保密性、软件容错、资源控制、剩余信息保护、抗抵赖。

数据安全：测评信息系统的数据安全保障情况，主要涉及对象为信息系统的管理数据及业务数据等。在内容上，数据安全层面测评实施过程涉及3个测评单元，包括：数据完整性、数据保密性、备份和恢复。

1. **安全管理测评**

安全管理制度：测评信息系统的安全管理制度情况。在内容上，安全管理制度方面测评实施过程涉及3个测评单元，包括：管理制度、制定和发布、评审和修订。

安全管理机构：测评信息系统的安全管理机构情况。在内容上，安全管理机构方面测评实施过程涉及5个测评单元，包括：岗位设置、人员配备、授权和审批、沟通和合作、审核和检查。

人员安全管理：测评信息系统的人员安全管理情况。在内容上，人员安全管理方面测评实施过程涉及5个测评单元，包括：人员录用、人员离岗、人员考核、安全意识教育和培训、外部人员访问管理。

系统建设管理：测评信息系统的系统建设管理情况。在内容上，系统建设管理方面测评实施过程涉及11个测评单元，包括：系统定级、安全方案设计、产品采购和使用、自行软件开发、外包软件开发、工程实施、测试验收、系统交付、安全服务商选择、系统备案、系统测评。

系统运维管理：测评信息系统的系统运维管理情况。在内容上，系统运维管理方面测评实施过程涉及13个测评单元，包括：环境管理、资产管理、介质管理、设备管理、网络安全管理、系统安全管理、恶意代码防范管理、密码管理、变更管理、备份与恢复管理、安全事件处置、应急预案管理、监控管理和安全管理中心。

1. **系统整体测评**

从信息系统整体上测评主要目的是分析是否能够对抗相应等级威胁的角度，对安全技术测评和安全管理测评中的不符合项和部分符合项进行综合分析，分析这些不符合项或部分符合项是否会影响到信息系统整体安全保护能力的缺失。信息系统的整体测评，就是在单元测评的基础上，评价信息系统的整体安全保护能力有没有缺失，是否能够对抗相应等级的安全威胁。

信息系统整体测评应从安全控制点间、层面间和区域间等方面进行安全分析和测评，并最后从系统结构安全方面进行综合分析，对系统结构进行安全测评。

# 项目整体清单预算

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **序号** | **产品/服务名称** | **数量** | **单价** | **总价** |
| **产品部分** | | | | |
|  | 核心交换机 | 2台 |  |  |
|  | 防火墙 | 1台 |  |  |
|  | 入侵检测系统 | 1台 |  |  |
|  | 网络准入控制系统 | 1台 |  |  |
|  | 安全管理中心SOC | 1台 |  |  |
|  | 安全态势感知平台 | 1太 |  |  |
|  | 运维管理审计系统（堡垒机） | 1台 |  |  |
|  | 数据库审计系统 | 1台 |  |  |
|  | 主机集中防病毒软件 | 1套（共约1+x+y） |  |  |
| **安全服务部分** | | | | |
|  | 定级备案协助 | X个X级系统 |  |  |
|  | 安全差距评估 | X个X级系统 |  |  |
|  | 安全整改设计 | X个X级系统 |  |  |
|  | 人工安全策略加固 | X个X级系统 |  |  |
|  | 管理制度建设与优化 | X个X级系统 |  |  |
|  | 等级保护验收测评 | X个X级系统 |  |  |