**国家保密局有关软硬件**

**采购项目**

**需求书**

**2020年6月**

**目录**

[第1章项目基本情况 1](#_Toc18332179)

[1.1项目背景 1](#_Toc18332180)

[1.2建设内容 1](#_Toc18332181)

[1.3项目投资及建设周期 1](#_Toc18332182)

[第2章软硬件一览表 2](#_Toc18332183)

[第3章采购服务交付、部署地点 4](#_Toc18332184)

[第4章技术需求 4](#_Toc18332185)

[4.1采购要求 4](#_Toc18332186)

[4.2工作内容 4](#_Toc18332187)

[第5章管理需求 5](#_Toc18332188)

[5.1服务质量要求 5](#_Toc18332189)

[5.2所有权和使用权 5](#_Toc18332190)

[5.3服务方式及人员要求 6](#_Toc18332191)

[第6章采购技术指标 8](#_Toc18332194)

# 第1章项目基本情况

## 1.1项目背景

本项目采购国家保密局有关软硬件。

## 1.2建设内容

1.采购交换机、防护系统等有关软硬件。

2.软硬件集成配合。配合总集成商，协调相关软硬件厂商，将采购的软硬件进行部署。

## 1.3项目投资及建设周期

本项目采购预算为190万元，合同签订后1个月内完成采购。如果整体建设周期因故延长，成交供应商不得因此提出增加费用的要求，请供应商充分考虑该风险因素。

# 第2章软硬件一览表

|  |  |  |
| --- | --- | --- |
| **序号** | **设备及软硬件名称** | **数量** |
| **一、网络系统** | | |
| 1 | 接入交换机 | 9台 |
| 2 | 汇聚交换机 | 2台 |
| 3 | 路由器 | 2台 |
| **二、存储系统** | | |
| 4 | 光纤交换机 | 2台 |
| 5 | A类磁盘阵列 | 1台 |
| 6 | 备份一体机 | 1台 |
| **三、终端及外设系统** | | |
| 7 | 测试专用移动工作站 | 9台 |
| 8 | 投影仪 | 5台 |
| **四、安全系统** | | |
| 9 | 千兆防火墙 | 1台 |
| 10 | 万兆防火墙 | 1台 |
| 11 | 接入控制网关 | 1套 |
| 12 | 主机漏洞扫描系统 | 1套 |
| 13 | web漏洞扫描系统 | 1套 |
| 14 | 入侵防御 | 1套 |
| 15 | 网络病毒防护系统 | 1套 |
| 16 | 运维审计 | 1套 |

详见第6章。

# 第3章采购服务交付、部署地点

产品安装和服务地点：国家保密科技测评中心指定办公区域

部署地点：国家保密科技测评中心指定办公区域

# 第4章技术需求

## 4.1采购要求

应对软硬件进行直采，不得将成交项目分包或转包给其他主体实施。确需分包的建设内容，需经建设方书面同意才可以执行。

## 4.2工作内容

（1）采购指标确认

制定采购方案，逐一与建设方确认采购指标，书面确认无误后，进行采购。

（2）软硬件采购

采购有关软硬件，配合建设方完成货物验收。

（3）软硬件集成配合

配合总集成商，协调有关软硬件厂商，将采购的软硬件部署至平台中。

（4）配合工程验收

配合完成竣工验收，配合完成审计。

**4.3售后服务**

项目竣工验收之日起3年内，提供7\*24小时电话支持服务；对采购的软硬件产品，采购人签发验收合格证书之日起3年内，提供免费质保服务3年，出现故障、质量问题的，成交供应商免费协助配合建设方进行更换、调试。

对于第2章中的A类磁盘阵列、备份一体机、千兆防火墙、万兆防火墙、主机漏洞扫描系统、web漏洞扫描系统、入侵防御类产品应提供原厂售后服务承诺（加盖原厂公章）。

# 第5章管理需求

## 5.1服务质量要求

(1)向建设方交付的实体货物必须是全新的、合法合规的，满足相关参数要求，并有相关合格证明。

(2)采购参数需调整的，应书面获取建设方同意后，方可实施采购。

(3)实施过程中积极开展相关组织协调工作，保证工程能够按时、保质、保量竣工。

## 5.2所有权和使用权

(1)硬件设备所有权

项目所采购硬件设备所有权全部归建设方。成交供应商保证，其有义务协助确保建设方采购货物的行为合法有效，建设方在中华人民共和国使用该货物或货物的任何一部分时，免受任何第三方提出侵犯其著作权、专利权、商标权、工业设计权等知识产权及其他权利的起诉，否则，成交供应商将承担相关责任。

(2)使用权

本项目所涉及的软件使用权归建设方所有。

## 5.3服务方式及人员要求

实施阶段，应协调相关厂商派员提供安装、调试等技术服务。

竣工验收阶段，驻场人员应不少于1名具有相关经验的人员负责驻场协助建设方、监理方进行竣工验收。驻场人员应为成交供应商正式人员，5年以上相关从业经验。

如实际驻场服务人员与磋商响应文件中承诺人员不符，建设方有权中止合同。磋商供应商应保证人员配置的合理性以及人员的稳定性，因人员的过失造成建设方的直接经济损失，应按照国家和行业相关规定赔偿建设方的损失。

## 5.4集成单位责任

**5.4.1**知识产权责任

本项目成交供应商有协助建设方进行合规采购的义务：确保所采购的第三方开发的硬件设备、软件产品，建设方拥有永久免费使用权以及在质保期内免费升级更新服务的权利。若建设方关于以上权利或权益受到收到相关起诉，成交供应商要承担相关责任。

**5.4.2其他责任**

(1)若成交供应商在项目实施过程中要更换项目人员，需向建设方提出书面申请，且更换的人员也应符合本项目关于各种人员的要求。

(2)如果因成交供应商工作失误，造成建设方经济损失的，成交供应商要按照国家和行业相关规定向建设方赔偿集成单位造成的损失。

(3) 成交供应商使用建设方提供的设备和物品属建设方所有，在成交供应商工作完成或终止时，应将设备和剩余物品按合同规定的时间和方式移交给建设方。

(4) 成交供应商要对项目人员的管理负责，若项目人员出现不按照建设方要求的行为，成交供应商应对其后果负责。

# 第6章采购技术指标

## （一）网络设备

### 1.接入交换机

| **序号** | **功能及指标项** | **技术指标要求** |
| --- | --- | --- |
| 1 | 硬件要求 | 交换机高度：1U  电源电压：AC：100V～240V；DC：-48～60V  端口结构：固定端口  端口数量：24个10/100/1000Base-T以太网端口，4个万兆SFP+  控制端口：1个Console口 |
| 2 | 功能要求 | 网络管理：支持Telnet远程配置、维护，支持SNMPv1/v2c/v3，支持RMON |
| 3 | 支持的特性：支持二层交换和三层路由 |
| 4 | 传输速率（bps）：≥100M/1000M/10000M |
| 5 | 包转发速率（pps）：108Mpps/126Mpps |
| 6 | 地址表容量：16K MAC |

### 2.汇聚交换机

| **序号** | **功能及指标项** | **技术指标要求** |
| --- | --- | --- |
| 7 | 硬件要求 | 交换机高度：1U  电源电压：AC：100V～240V；DC：-48～60V  端口结构：固定端口  端口数量：不少于24个  控制端口：1个Console口  扩展模块：可扩展40GE接口 |
| 8 | 功能要求 | 支持二层交换和三层路由 |
| 9 | 支持远程配置、维护 |
| 10 | 传输速率（bps）：≥100M/1000M/10000M/40000M |
| 11 | 包转发速率（pps）：444 Mpps |
| 12 | 地址表容量：32K MAC |
| 13 | 背板带宽（bps）：680 Gbps/6.8 Tbps |

### 3.路由器

| **序号** | **功能及指标项** | **技术指标要求** |
| --- | --- | --- |
| 14 | 硬件要求 | 3GE WAN(1GE Combo),2 USB,4 SIC,2 WSIC,150W交流电源  控制端口：1个Console口 |
| 15 | 功能要求 | 包转发率：≥9Mpps |
| 16 | VPN：支持 |
| 17 | QoS：支持 |
| 18 | 网管功能：支持 |
| 19 | 支持3\*GE (1\*Combo) |

## （二）存储系统

### 4.光纤交换机

| **序号** | **功能及指标项** | **技术指标要求** |
| --- | --- | --- |
| 20 | 硬件要求 | 交换机高度：1U  电源电压：AC：100V～240V；DC：-48～60V  控制端口：1个Console口 |
| 21 | 功能要求 | 支持二层交换和三层路由 |
| 22 | 支持Telnet远程配置、维护，支持SNMPv1/v2c/v3 |
| 23 | 传输速率（bps）：≥100M/1000M/10000M/40000M |
| 24 | 包转发速率（pps）：≥444 Mpps |
| 25 | 地址表容量：32K MAC |

### 5.A类磁盘阵列

| **序号** | **功能及指标项** | **技术指标要求** |
| --- | --- | --- |
| 26 | 硬件要求 | 4端口 10Gb端口联合扩展卡 1.2TB SAS 10K 2.5英寸硬盘 安装服务 硬盘数量：4 |
| 27 | 功能要求 | 最大支持存储容量：1000 TiB |
| 28 | 控制器数量：2 |
| 29 | 接口主机：4×16 Gbps FC，8×10Gb |
| 30 | 缓存数量：64GB |
| 31 | 混插功能：支持 |
| 32 | 预装正版软件，提供软件著作权证书 |

### 6.备份一体机

| **序号** | **功能及指标项** | **技术指标要求** |
| --- | --- | --- |
| 33 | 硬件要求 | 2U（含导轨）机架式软硬一体化设备，内置高速SSD系统盘；支持12盘位；配置冗余电源；系统硬盘2\*240GB；备份硬盘不小于24T。 |
| 34 | 功能要求 | 采用分布式存储架构，可按需无缝横向扩展存储介质服务器；单个系统可支持64台存储介质服务器同时执行备份任务，每台介质服务器可以分别承担不同的传输任务性；提升整体备份效率。 |
| 35 | 系统采用可信灾备架构设计，备份时可选择商密AES算法和国密SM系列算法对备份对象进行源端加密，备份集要求以SSL或HTTPS等安全协议进行传输，备份集以指定非对称密钥进行加密存储，数据恢复时可选择数字证书认证方式进行解密恢复，数字证书认证时提供单一方式或3选2方式进行认证登录，确保灾备全程安全可信。 |
| 36 | 支持文件级CDP和卷级CDP的双重持续保护技术，提供IO级细颗粒度数据保护，而非准CDP或快照技术；CDP间隔≤1秒，并可在系统中输入任意1秒进行数据恢复，解决数据丢失和数据逻辑错误问题； |
| 37 | 支持Oracle、SQL Server、MySQL、DB2、达梦、人大金仓、南大通用、神通数据库等国内主流数据库的在线定时和实时备份保护；支持对国产涉密专用服务器相关数据进行备份。 |
| 38 | 支持数据直接备份至系统存储介质中，无需生产机单独提供日志卷作为CDP缓存区，以防缓存卷因空间不足而导致备份任务中断或生产机没有单独的日志缓存卷造成的部署困难。 |
| 39 | 支持以非脚本的方式对数据库进行保护； |
| 40 | 支持Windows、Linux、HP-Unix、中标麒麟、凝思磐石、银河麒麟、普华系统、红旗Linux等国内外主流操作系统的在线热备份保护；要求初始化备份采用完全备份，后期采用差量备份； |
| 41 | 支持对FusionSphere、CAS、Openstack、Hyper-V的无代理方式备份保护 |
| 42 | 支持集群环境下的VMware虚拟化平台无代理备份保护模式，无需在任意虚机中安装客户端代理，无需寻找其它任意备份代理服务器，可以实现直接挂在使用、文件级细粒度恢复。 |
| 43 | 支持主流蓝光存储设备，支持将备份数据通过蓝光光盘进行离线归档保存，支持D2D2B； |
| 44 | 支持一对一、一对多以及多对一等多种异地灾备，最大限度满足多分支机构的异地数据灾备需求。支持本地恢复及异地恢复； |
| 45 | 当数据备份过程中出现链路中断，恢复正常后，可从上一次断点处继续增量传输数据，无需重新进行完整数据传输，确保灾备数据的传输效率和完整性。 |
| 46 | 支持以AES256位加密算法对备份数据进行加密；可以以密码验证方式对灾备保护的数据进行恢复操作 |
| 47 | 支持千万级以上海量文件日志增量备份保护，可快速定位到修改或新增的文件并进行备份，无须每次增量备份时扫描所有文件；增量备份间隔可达分钟级； |
| 48 | 支持三权分立管理模式，即：系统管理员、审计管理员、安全管理员三种管理员身份多权限、多角色管理； |

## （三）终端及外设系统

### 7.测试专用移动工作站

| **序号** | **功能及指标项** | **技术指标要求** |
| --- | --- | --- |
| 49 | 硬件要求 | 显示器尺寸：15.6英寸；分辨率：FHD1920\*1080；CPU：酷睿i7-6820HQ 4核（主频≥2.7Ghz，缓存容量(各级缓存容量之和9.25）或更好；硬盘：≥512GB 固态硬盘1TB 接口类型SATA；内存：≥16G DDR4；2个内存插槽；显卡类型：独立显卡，显存容量≥4G ；光驱类型：DVDRW USB（外置）；无线网卡：802.11a/b/g/n/ac/有线网卡：10/100/1000M自适应/WIN7专业版操作系统/鼠标：有线USB接口/电脑包、鼠标/电池90WH/ |

### 8.投影仪

| **序号** | **功能及指标项** | **技术指标要求** |
| --- | --- | --- |
| 50 | 硬件指标 | 输入端子：HDMI x2，USB 3.0 x1，USB 2.0 x1，AC in x1，Mini USB\*1  输出端子：S/PDIF x1  USB接口：USB2.0\*1,USB3.0\*1,Mini USB\*1；  HDMI接口：HDMI\*2；  光学规格：高压汞灯；  亮度(流明)：≥3500ANSI；  标准分辨率：≥1920X1080dpi；  兼容最大分辨率：1080P，4K；  对比度：3001-5000:1；  投影光源：超高压汞灯泡；  显示技术：DLP |
| 51 | 放映指标 | ±45°四向梯形矫正，灯泡寿命≥4000小时;  网络接口:以太网\*1;音频接口:S/PDIF x1;其他接口:AC in\*1;  支持H.264 4K/2k 30fps格式解码; |

## （二）安全系统

### 9.千兆防火墙

| **序号** | **功能及指标项** | **技术指标要求** |
| --- | --- | --- |
| 52 | 硬件要求 | 机箱：1U机箱 拓展槽数量：≥2个可插拔扩展槽 |
| 53 | 电口数量：≥6个10/100/1000BASE-T 千兆光口数量:≥2个SFP口 |
| 54 | 性能要求 | 整机吞吐：≥4Gbps |
| 55 | 并发连接数：≥220万 |
| 56 | 支持路由、交换、混合、虚拟线工作模式； |
| 57 | 支持静态路由、ISP路由及动态路由协议，支持802.1q、QinQ模式； |
| 58 | 为提高链路可靠性，需支持手工链路聚合及LACP链路聚合，支持不少于10种的负载分担算法。 |
| 59 | 支持手动添加绑定，基于IP、接口的动态探测绑定，支持跨三层IP/MAC绑定，IP/MAC绑定表可导入导出； |
| 60 | 支持智能DNS及DNS Docting功能，同时支持通过配置多条 DNS Doctoring，实现内网资源服务器的负载均衡。 |
| 61 | 支持IPv4/IPv6双栈工作模式； |
| 62 | 支持IPv6安全控制策略设置，能针对IPv6的目的/源地址、目的/源服务端口、区域、服务、时间、扩展头属性等条件进行安全访问规则的设置。 |
| 63 | 内置用户身份管理系统，支持本地认证、证书认证及免认证等方式，同时支持RADIUS、LDAP、TACACS等多种第三方外部认证设置； |
| 64 | 综合运用身份认证与访问控制技术，实现基于用户身份的安全防护策略部署与可视化监控； |
| 65 | 支持本地CA和第三方CA，可作为CA认证中心或采用第三方CA为他人签发证书。 |
| 66 | 支持在同一条访问控制策略中配置传统的五元组信息、用户、域名、应用、服务、时间的识别与控制； |
| 67 | 提供智能策略分析功能，支持策略命中分析、策略冗余分析、策略冲突检查，可在WEB界面显示检测结果。 |
| 68 | 支持黑名单功能，可设置多个对象条件，如：五元组信息、地址范围、应用、用户等； |
| 69 | 内置流量检测清洗引擎，支持基于IP、ICMP、TCP、UDP、DNS、HTTP、NTP等众多协议类型的防护策略； |
| 70 | 支持根据DOS/DDOS攻击行为自动添加动态黑/白名单功能，可自定义动态黑/白名单超时时间； |
| 71 | 支持在WEB界面进入CLI模式，执行系统配置、网络诊断、过滤抓包等命令。 |
| 72 | 支持多条日志合并传送，支持日志传输加密； |
| 73 | 日志留存期限半年以上 |
| 74 | 系统具有相互独立的系统管理员、安全保密管理员和安全审计员，符合保密局规范的管理员“三权分立”功能。 |
| 75 | 产品资质要求 | 信息技术产品安全测评证书（EAL3+） |
| 76 | 符合国家保密标准和规范要求，具有国家保密科技测评中心出具的产品检测证书 |

### 10.万兆防火墙

| **序号** | **功能及指标项** | **技术指标要求** |
| --- | --- | --- |
| 77 | 硬件要求 | 机箱：2U机箱 拓展槽数量：≥3个可插拨扩展槽 |
| 78 | 电口数量：≥2个10/100/1000BASE-T 万兆光口数量:≥2个SFP＋口 |
| 79 | 性能要求 | 整机吞吐：≥36Gbps |
| 80 | 并发连接数：≥800万 |
| 81 | 支持路由、交换、混合、虚拟线工作模式； |
| 82 | 支持静态路由、ISP路由及动态路由协议，支持802.1q、QinQ模式； |
| 83 | 为提高链路可靠性，需支持手工链路聚合及LACP链路聚合，支持不少于10种的负载分担算法。 |
| 84 | 支持手动添加绑定，基于IP、接口的动态探测绑定，支持跨三层IP/MAC绑定，IP/MAC绑定表可导入导出。 |
| 85 | 支持智能DNS及DNS Docting功能，同时支持通过配置多条 DNS Doctoring，实现内网资源服务器的负载均衡。 |
| 86 | 支持IPv4/IPv6双栈工作模式； |
| 87 | 支持IPv6安全控制策略设置，能针对IPv6的目的/源地址、目的/源服务端口、区域、服务、时间、扩展头属性等条件进行安全访问规则的设置。 |
| 88 | 内置用户身份管理系统，支持本地认证、证书认证及免认证等方式，同时支持RADIUS、LDAP、TACACS等多种第三方外部认证设置。 |
| 89 | 综合运用身份认证与访问控制技术，实现基于用户身份的安全防护策略部署与可视化监控； |
| 90 | 支持本地CA和第三方CA，可作为CA认证中心或采用第三方CA为他人签发证书。 |
| 91 | 支持在同一条访问控制策略中配置传统的五元组信息、用户、域名、应用、服务、时间的识别与控制； |
| 92 | 提供智能策略分析功能，支持策略命中分析、策略冗余分析、策略冲突检查，可在WEB界面显示检测结果。 |
| 93 | 支持黑名单功能，可设置多个对象条件，如：五元组信息、地址范围、应用、用户等； |
| 94 | 内置流量检测清洗引擎，支持基于IP、ICMP、TCP、UDP、DNS、HTTP、NTP等众多协议类型的防护策略； |
| 95 | 支持根据DOS/DDOS攻击行为自动添加动态黑/白名单功能，可自定义动态黑/白名单超时时间； |
| 96 | 支持在WEB界面进入CLI模式，执行系统配置、网络诊断、过滤抓包等命令。 |
| 97 | 支持多条日志合并传送，支持日志传输加密； |
| 98 | 日志留存期限半年以上 |
| 99 | 系统具有相互独立的系统管理员、安全保密管理员和安全审计员，符合保密局规范的管理员“三权分立”功能。 |
| 100 | 产品资质要求 | 信息技术产品安全测评证书（EAL3+） |
| 101 | 符合国家保密标准和规范要求，具有国家保密科技测评中心出具的产品检测证书 |

### 11.接入控制网关（网络准入）

| **序号** | **功能及指标项** | **技术指标要求** |
| --- | --- | --- |
| 102 | 硬件要求 | 机箱：2U 电源：双电源 拓展槽数量：≥2个 |
| 103 | 电口数量：≥6个 |
| 104 | 千兆光口数量:≥2个SFP插槽 |
| 105 | 性能要求 | 最大用户数：≥1000个 |
| 106 | 功能要求 | 支持旁路或串联部署，串联部署采取透明网关准入模式时不依赖于交换机、路由器以及防火墙等设备，避免对已有网络进行较大规模的调整 |
| 107 | 支持双操作系统冷备，当常用系统出现故障可以使用备用系统恢复。 |
| 108 | 具备单机模式下的系统逃生工具，可添加维护交换机信息，在准入设备故障时进行自动或手动方式逃生 |
| 109 | 支持命令行与B/S模式管理，提供系统首页图形化展示功能，可展示设备面板状态、CPU状态、内存状态、硬盘状态、在线用户、报警统计等信息。 |
| 110 | 支持802.1X、Portal、透明网关、策略路由等多种准入模式选择，单设备情况下可进行混合准入模式应用。 |
| 111 | 提供手机短信认证方式，可与短信服务器联动，在终端入网认证时下发验证码 |
| 112 | 支持信息绑定认证，可检查入网终端IP、终端MAC、用户名、交换机IP、交换机端口、终端硬件ID等多要素信息 |
| 113 | 支持同账户多在线管理，能够对同一用户同时刻允许使用终端数进行限制，处理方式包括：下线第一个、下线最后一个、不处理等。 |
| 114 | 支持黑/白名单管理，可根据所应用的不同准入模式，设置黑/白名单终端IP、MAC、协议、端口、VLAN号等信息 |
| 115 | 支持IP冲突管理，对入网终端与已在线终端IP冲突时提供处理方式，方式包括：下线已在线终端及不处理等 |
| 116 | 支持认证用户管理，可创建组织结构并添加用户信息，信息包括登录名、姓名、密码、单位、电话、办公地址、邮箱、VLAN ID、ACL规则名等信息，可进行批量导入导出 |
| 117 | 支持资产管理功能，可添加、修改、删除资产信息，资产类型包括：台式机、笔记本、打印机、IP电话机、服务器、工作站、手机等，并可对不同资产实施MAC免认证操作 |
| 118 | 图形化显示系统磁盘状态信息，内容包括：资产数据、报警日志、日志文件、用户数据、对象和策略、其他数据、空闲磁盘空间等，并列出所占空间大小，支持系统磁盘数据的备份、恢复、清理，可按照不同数据对象、时间对象进行系统自动备份操作。 |
| 119 | 支持系统当前状态进行诊断分析，展示不同准入模式运行状态、服务是否正常，并提供系统调试、抓包分析等功能 |
| 120 | 产品资质要求 | 提供国家信息安全测评信息技术产品安全测评证书（EAL3+级）证明材料 |
| 121 | 符合国家保密标准和规范要求，具有国家保密科技测评中心出具的产品检测证书。 |

### 12.主机漏洞扫描系统

| **序号** | **功能及指标项** | **技术指标要求** |
| --- | --- | --- |
| 122 | 硬件要求 | 1\*RJ45串口，1\*GE管理口，5个10M/100M/1000M自适应以太网电口扫描口。标准配置提供1路授权扫描端口 |
| 123 | 功能要求 | 支持模版自动匹配、信息重整化技术、端口服务智能识别、OpenVM等技术 |
| 124 | 采用B/S管理架构，能够以SSL加密通讯方式通过浏览器来远程进行管理，无需额外安装控制台 |
| 125 | 系统能够支持多级分布式部署，通过管理节点可以对多台子节点进行管理 |
| 126 | 系统采用经过精简和安全优化的嵌入式安全操作系统 |
| 127 | 产品支持手动升级和自动升级，本地升级和在线升级方式，升级周期固定周期为两周，重大漏洞与国际厂商同步 |
| 128 | 能够对Windows系列、Linux、AIX、HPUX、IRIX、BSD、Solaris等主流操作系统、网络设备、数据库和应用系统等进行漏洞扫描。 |
| 129 | 符合国家保密标准和规范要求，具有国家保密科技测评中心出具的产品检测证书。 |

### 13.WEB漏洞扫描系统

| **序号** | **功能及指标项** | **技术指标要求** |
| --- | --- | --- |
| 130 | 硬件要求 | 1U机型，含交流单电源，1\*RJ45串口，1\*GE管理口，4个10M/100M/1000M自适应以太网电口扫描口，4个千兆SFP插槽。 |
| 131 | 功能要求 | 采用B/S管理架构，支持多级分布式部署，通过管理节点可以对多台子节点进行管理 |
| 132 | 提供详细的漏洞描述和对应的解决方案描述 |
| 133 | 漏洞知识库与CVE、CNCVE、CNNVD、CNVD、CVSS等主流标准兼容 |
| 134 | 支持的SQL注入涵盖“字符型、数字型、搜索型”等在内的及其变形的SQL注入方式 |
| 135 | 并且支持基于POST、GET、Cookie方式来提交数据 |
| 136 | 可以绕过普通过滤强度的注入过滤代码，支持Cookie注入、XSS检测、Cookie有效性检测, 系统能够检测出不低于20种基于GET请求、POST请求的跨站攻击方法及变种, 支持伪造跨站点请求检测；支持网页挂马检测 |
| 137 | 支持隐藏字段检测；分析器支持常见的字符编码标准 |
| 138 | 支持Web服务漏洞的检查。支持WAP站点扫描；支持基于HTTPS应用系统的扫描；支持ERP等复杂的Web应用系统扫描 |
| 139 | 支持易通、织梦、DEDECMS、Discuz、Ecshop、易思、大汉、PHPCMS、PHP168、PHPCMS2008、phpcms v9、SHOPEX、Nginx代码执行、Spring代码执行等国内、国外知名WEB应用程序漏洞扫描 |
| 140 | 支持Oracle、SQL Server、DB2、Informix、Sybase、MySQL、PostgreSQL、Access等后台数据库类型 |
| 141 | 符合国家保密标准和规范要求，具有国家保密科技测评中心出具的产品检测证书 |

### 14.入侵防御

| **序号** | **功能及指标项** | **技术指标要求** |
| --- | --- | --- |
| 142 | 硬件要求 | 需至少选配1个接口板卡。2U上架设备，1个RJ-45 Console口，1个10/100/1000 Base-T带外管理口，2个10/100/1000 Base-T HA口，4个网络接口板扩展槽位，2个USB口，双电源。 |
| 143 | 功能要求 | 具备融合模式匹配、协议分析、异常检测、会话关联分析，以及抗IDS/IPS逃逸等多种技术，准确识别各种黑客入侵，为用户提供2~7层深度入侵防御 |
| 144 | 提供覆盖广泛的攻击特征库，能够针对7600种以上的攻击行为、异常事件，以及网络资源滥用流量，进行检测和防御 |
| 145 | 携带的攻击特征库须获得CVE-Compatible兼容性认证。提供基于流的应用识别技术，可准确识别非标准端口应用、以及HTTP协议隧道中Web2.0应用，发现隐藏在应用中的攻击行为 |
| 146 | 提供对网络病毒、蠕虫、间谍软件、木马后门、刺探扫描、暴力破解等恶意流量的检测和阻断 |
| 147 | 融合协议异常检测能力，有效抵御缓冲区溢出攻击，以及各类未知攻击 |
| 148 | 具备零日攻击防护能力，保护用户避免遭受新的安全威胁。能够有效抵御SQL注入、僵尸网络等多种常见的应用层安全威胁 |
| 149 | 提供先进的DoS/DDoS攻击防护能力，支持双向阻断TCP/UDP/ICMP/ACK Flooding，以及UDP/ICMP Smurfing等常见的DoS/DdoS的攻击 |
| 150 | 能够基于敏感数据的外泄、文件识别、服务器非法外联等异常行为检测，实现内网的高级威胁防护功能 |
| 151 | 提供入侵行为和应用软件特征的自定义接口，可根据用户需求定制对其它流量的检测和阻断规则 |
| 152 | 产品资质要求 | 符合国家保密标准和规范要求，具有国家保密科技测评中心出具的产品检测证书 |

### 15.网络病毒防护系统

| **序号** | **功能及指标项** | **技术指标要求** |
| --- | --- | --- |
| 153 | 硬件要求 | 标配6个10/100/1000M电口；或可配光口，可扩展最多12个光口 |
| 154 | 功能要求 | 可支持双归属链路网络部署，采用非传统sock代理处理模式，数据处理性能更高 |
| 155 | 具备优良的网络适应性以及，支持对HTTP、SMTP、POP3、IMAP、FTP等协议上的各类病毒查进行有效查杀，保护网络安全 |
| 156 | 支持快速扫毒和全面扫毒两种扫毒模式，支持压缩格式文件查杀，病毒特征数量大于600万 |
| 157 | 支持对HTTP、FTP 及各种邮件传输协议流量和压缩文件（zip，gzip，rar等）中病毒的查杀 |
| 158 | 可有效拦截/监控诸如病毒传播、蠕虫攻击、木马通讯、僵尸网络、口令探测等当前活跃的多种网络威胁 |
| 159 | 综合采用数据包结构分析、网络行为分析、特征识别、模式匹配、流量控制与自动抑制、协议分析、深度内容分析、专业防病毒识别、蠕虫过滤、木马通讯阻断、口令嗅探识别、全透明桥接等技术，实现对网络威胁数据的精确过滤 |

### 16.运维审计（堡垒机）

| **序号** | **功能及指标项** | **技术指标要求** |
| --- | --- | --- |
| 160 | 硬件要求 | 机箱：1U机箱；存储空间：≥1T存储空间； |
| 161 | 接口数量：1个console口，2个USB口；≥4个10/100/1000BASE-T；；拓展槽数量：≥1个可插拨扩展槽 |
| 162 | 性能要求 | 授权许可：≥50个主机/设备许可用户数不限制 |
| 163 | 功能要求 | 支持旁路单臂部署，以逻辑网关方式工作；不改变现有网络结构，不改变运维人员的运维习惯； |
| 164 | 不限级数的进行分层分级分类管理；支持从AD域抽取OU，方便快速建立组织结构 |
| 165 | 资源分组支持以树形方式展现，不限制分组层级数量；资源类型支持unix资源、网络资源、windows资源、数据库资源、C/S资源、B/S资源、中间件资源、大型机资源等 |
| 166 | 资源授权模式基于岗位授权，岗位上绑定资源账号，这样授权可迁移、授权粒度更细；并可针对岗位设置相关安全策略 |
| 167 | 运维人员可将经常访问的资源添加到收藏夹，根据自己的登录习惯，更加便捷的定位需要访问的资源。 |
| 168 | 支持一键批量登录选中的资源，简化工作量；支持将登录配置保存为默认后，可以一键快速登录目标资源。 |
| 169 | 支持RDP-Tcp属性中的所有功能配置，包括加密级别为客户端兼容、低、高、符合FIPS标准等加密级别 |
| 170 | 自身提供证书认证服务，也可与第三方CA、动态令牌、生物识别、短信认证等方式进行结合。支持组合认证，提高访问的安全性。 |
| 171 | 支持上下行剪切板控制、共享磁盘控制、控制台登录控制 |
| 172 | 支持字符命令操作的黑白名单设置，命令权限控制规则应支持正则表达式，并可以对命令的参数进行限制并记录日志 |
| 173 | 支持对RDP实时会话的锁定和解锁，并可以在锁定解锁时发送即时通讯消息。发现危险操作可立即进行锁定操作 |
| 174 | RDP审计策略支持关键帧，帧间隔，录像文件压缩比等设置，以缩小录像文件大小；支持审计录像的画质选择，至少支持真彩，伪真彩，灰度三种画质选择。 |
| 175 | 对字符命令方式的访问可以审计到所有交互内容，可以还原操作过程的命令输入和结果输出，并且可以高亮显示高危命令 |
| 176 | 支持将重要的资源设置为登录审批，登录访问是需提交工单申请，审批人同意才可登录 |
| 177 | 支持将高危命令设置为执行需审批策略，当指定资源执行高危命令时，需要审批通过后，命令才能执行生效； |
| 178 | 系统预设常用统计报表模板，分为基础业务报表、行为审计报表、信息管理报表三大类。报表提供Word、Excel、PDF类型下载，支持按单次、周、月定时周期性生成，并且支持将生成报表发送到指定邮箱； |
| 179 | 支持日志数据的外置存储备份，支持NFS和windows文件共享协议，远程审计存储和本地存储对审计员透明； |
| 180 | 产品资质要求 | 符合国家保密标准和规范要求，具有国家保密科技测评中心出具的产品检测证书 |