采购需求(二次)

一、项目名称

三亚市公安局信息系统安全建设

其中：A 包：软硬件设备及材料采购

B 包：等级保护测评及信息安全服务

二、项目概况

该项目的主要建设内容是建立三亚市公安局三张网络的总体信息安全等级保护体系，根据等保要求，三亚市公安局的信息安全体系建设将包括以下几个方面：

1、公安网区域安全建设

2、互联区域安全建设

3、视频专网区域安全建设

4、安全管理体系建设

本期项目主要是对三亚市公安局的公安网、互联网、视频专网部分进行安全建设、策略优化及相应安全服务，建设内容包括网络架构调整、区域规划、设备购置、网站防护、加固指导、管理体系建设、应急预案及应急演练服务、安全渗透及等保测评等。

本项目中预算为 3,682,856 元，包含软硬件采购、等级保护测评及信息安全服务费，各标段预算分述如下：

1、软硬件设备及材料采购（A 包）：¥3,122,856.00 元

2、等级保护测评及信息安全服务（B 包）：¥560,000.00 元

用户需求书（A 包）

一、项目名称

软硬件设备及材料采购

二、采购清单

主要采购的软硬件设备包括：防火墙、WEB 防火墙、防毒墙、准入控制、运维审计、数据库审计、日志审计及网管平台等，具体清单如下：

序号	名　称	单位	数量	备注
一、公安网				
1	上联边界防火墙	台	1	
2	服务器区域边界防火墙	台	1	
3	上联边界防毒墙	台	1	
4	终端准入控制系统	台	1	
5	运维审计系统	套	1	
6	数据审计系统	套	1	
7	日志审计系统	套	1	
8	网络管理平台	套	1	
9	网络管理平台服务器	台	1	
二、视频专网				
1	边界防火墙	台	1	
2	终端准入控制系统	台	1	
3	运维审计系统	套	1	
4	日志审计系统	台	1	
5	网络管理平台	套	1	
6	网络管理平台服务器	台	1	
7	服务器接入交换机	台	2	
三、互联网				
1	边界防火墙	台	1	
2	边界 WEB 防火墙	台	1	
3	终端准入控制系统	台	1	
4	服务器接入交换机	台	1	

三、详细技术参数及技术要求

注：以下参数中带▲的参数为重要参数，如不满足则将在评分中加重扣分。

1、公安网

（1）上联边界防火墙

序号	指标项	技术参数及技术要求
1	▲基本配置	双冗余电源；≥6 个 10/100/1000M Base-TX 接口，≥4 个 SFP 接口；

		最大并发连接数≥300 万，最大吞吐量≥10Gbps，每秒新建连接数≥8 万；
		配置 IPS 模块，含三年特征库升级
2	网络适应性	支持静态路由，动态路由（OSPF、RIP 等），VLAN 间路由，单臂路由等。
3	网络管理	支持 DHCP Client、DHCP Relay、DHCP Server。
		支持链路聚合功能，支持静态轮询、热备等多种模式。
		支持基于数据包的安全域、地址、用户及用户组、MAC、端口号、服务、域名等进行安全策略控制 。
		支持策略命中数显示。
		支持根据 IP 地址进行策略查询、支持根据服务端口进行策略查询。
4	入侵防护	支持基于策略的入侵检测与防护，可针对不同的源目 IP 地址、服务、用户等，采用不同的入侵防护策略。
		入侵防御特征库库包括信息窃取、木马后门、间谍软件、可疑行为、网络设备攻击、安全漏洞及网络数据库攻击等的特征事件。
		支持细粒度的自定义 IPS 特征功能。
		支持对网络扫描行为的检测和过滤，可实现基于端口的扫描防护和基于主机的扫描防护。
		支持 IP/MAC 地址绑定的方式防止 ARP 欺骗。
		支持丢弃封包、切断会话、攻击重定向、记录日志等响应方式。
		支持实时的入侵防护事件分级报警列表，可按事件的源 IP、目的 IP、协议、时间等显示。
5	统一认证管理	支持多人使用同一帐号登录。
		支持对 WEB 认证、LDAP 认证、RADIUS 认证。
		支持用户口令复杂度设置。
		支持显示详细的用户在线信息，包括用户名称、登录 IP/MAC、在线时间、登录时间等。
6	主动防御	支持 IPv4 和 IPv6 双栈协议下的主动防御。
7	安全日志	支持中文日志记录。
		支持对日志文件的导出/导入
8	高可用性	可在热备和集群工作模式下支持多台防火墙的会话、配置的实时同步、手动同步。
		支持基于 VRRP 技术的热备和负载均衡。
		在 NAT、路由、透明模式下支持 A-A,A-S 模式。
9	▲保修	三年原厂硬件质保

（2）服务器区域边界防火墙

序号	指标项	技术参数及技术要求
1	▲基本配置	双冗余电源；≥6 个 10/100/1000M Base-TX 接口，≥4 个 SFP 接口；
		最大并发连接数≥300 万，最大吞吐量≥8Gbps，每秒新建连接数≥6 万；
		配置 IPS 模块、AV 模块，含三年特征库升级
2	网络适应性	支持静态路由，动态路由（OSPF、RIP 等），VLAN 间路由，单臂路由等。
3	网络管理	支持 DHCP Client、DHCP Relay、DHCP Server。
		支持链路聚合功能，支持静态轮询、热备等多种模式。
		支持基于数据包的安全域、地址、用户及用户组、MAC、端口号、服务、

		域名等进行安全策略控制 。
		支持策略命中数显示。
		支持根据 IP 地址进行策略查询、支持根据服务端口进行策略查询。
4	入侵防护	支持基于策略的入侵检测与防护，可针对不同的源目 IP 地址、服务、用户等，采用不同的入侵防护策略。
		入侵防御特征库库包括信息窃取、木马后门、间谍软件、可疑行为、网络设备攻击、安全漏洞及网络数据库攻击等的特征事件。
		支持细粒度的自定义 IPS 特征功能。
		支持对网络扫描行为的检测和过滤，可实现基于端口的扫描防护和基于主机的扫描防护。
		支持 IP/MAC 地址绑定的方式防止 ARP 欺骗。
		支持丢弃封包、切断会话、攻击重定向、记录日志等响应方式。
		支持实时的入侵防护事件分级报警列表，可按事件的源 IP、目的 IP、协议、时间等显示。
5	恶意代码防护	支持基于策略的病毒扫描与防护，可针对不同的源目 IP 地址、源 MAC 地址、服务等，采用不同的病毒防护策略。
		支持应用协议自识别，可以实现 HTTP,SMTP,FTP,POP3,IMAP,FTP,WEBMAIL 多种应用协议下的病毒防护，支持自定义非标准端口下应用协议的病毒防护。
		支持常见 WEB 邮件系统的病毒防护。
		支持路由、透明、混合等各种工作模式下的网络病毒检测。
		支持隔离病毒源地址，防止病毒源主机访问内部网络，提高网络整体安全性。
		系统内置多种病毒防护模板，支持自定义病毒防护模板。
		支持过滤邮件病毒、文件病毒、恶意网页代码、木马后门、蠕虫等多种类型的病毒。
6	统一认证管理	支持多人使用同一帐号登录。
		支持对 WEB 认证、LDAP 认证、RADIUS 认证。
		支持用户口令复杂度设置。
		支持显示详细的用户在线信息，包括用户名称、登录 IP/MAC、在线时间、登录时间等。
7	主动防御	支持 IPv4 和 IPv6 双栈协议下的主动防御。
8	安全日志	支持中文日志记录。
		支持对日志文件的导出/导入
9	高可用性	可在热备和集群工作模式下支持多台防火墙的会话、配置的实时同步、手动同步。
		支持基于 VRRP 技术的热备和负载均衡。
		在 NAT、路由、透明模式下支持 A-A,A-S 模式。
10	▲保修	三年原厂硬件质保

3、上联边界防毒墙

序号	指标项	技术参数及技术要求
1	▲硬件要求	冗余电源，≥4 个 10/100/1000MBase-T 端口，≥4 个 SFP 端口。设备硬件 Bypass≥2 路。

2	▲性能要求	最大并发连接数≥300 万，最大吞吐量≥10Gbps，每秒新建连接数≥8 万。
3	▲产品形态	产品为软硬件一体化的专业防毒墙
		产品对通过文件、邮件附件、网页浏览等方式传播的木马、病毒、后门、蠕虫、间谍软件等恶意软件实时扫描并拦截，同时可分析网内各种应用协议使用情况，以及防御 SQL 注入、XSS 跨站脚本等针对 WEB 服务器的攻击。
4	功能要求	支持对 HTTP/HTTPS/FTP/SMTP/POP3 等协议实现木马、病毒、后门、间谍软件、蠕虫等恶意软件的扫描和过滤。
		设备支持基于端口的 VLAN 和基于 802.1Q 的 VLAN。
		支持僵尸网络的防护。
		支持恶意网页和 URL 过滤功能，并支持自定义黑白名单。
		支持直连病毒预防模式或旁路病毒预警部署模式。
		支持详细的病毒防护日志记录，包括记录日期、病毒名、文件名、源 IP 地址、目的 IP 地址、采取的动作等内容。
		支持即时、定期报表生成功能，体现病毒威胁变化、当前会话数、系统运行状态信息等。
		支持简体中文操作界面和多级管理员权限分配。
		支持带内、带外管理，可通过 SSL 加密的 WEB 、SSH 命令行、Console 方式管理。
5	▲保修	三年特征库升级，三年原厂硬件质保

（4）终端准入控制系统

序号	指标项		技术参数及技术要求
1	基本要求	▲系统要求	具有独立自主知识产权，须为标准机架式硬件产品，除自身硬件设备外，产品功能的实现无需额外增加服务器等设备。具备桌面安全管理功能。
		▲硬件要求	采用标准机架式硬件设备，千兆电口≥6 个
		▲性能要求	每秒事务数（TPS）≥3500（次/秒），最大吞吐量≥1.5Gbps，最大并发链接数≥3000（条）；用户许可≥1500。
		高可用性	准入设备具备 HA 模式，HA 支持主备机心跳 IP 检测及虚地址管理模式，支持 vrrp 管理模式。
			提供第三方监控平台，在出现重大异常情况时能及时通知网络设备放开网络。
		终端部署	准入设备至少提供安全客户端（Agent）、安全控件、无客户端等多种可供自定义部署、管理模式。
			安全客户端模式部署时，客户端程序应支持功能定制，以降低系统资源耗用，提升客户端兼容性。
2	准入架构	终端发现	能够实时监测并发现接入内网的 PC、平板电脑、智能手机、IP 设备等终端，能够在第一时间隔离阻断并通知管理员。

			对自动发现的终端能够按照类别自动归类，以方便网络终端的统计管理（提供截图证明，加盖原厂商章）。
		准入技术	准入设备原生支持 802.1x 标准协议，无需第三方 RADIUS 服务器支持。
			▲准入设备支持基于多厂商 Virtual Gateway 的 VLAN 隔离技术，实现无客户端环境下端口级准入控制（提供截图证明，加盖原厂商章）。
			▲准入控制设备支持不少于 3 种准入技术，并可以提供同时使用（提供截图证明，加盖原厂商章）。
			准入设备支持基于策略路由技术的准入控制模式，入网设备在访问网内关键资源时，将被强制隔离、引导至认证管理页面，同时支持交换机接口动态 VLAN 下发、端口隔离模式的网络边界管理。
			单台准入设备可支持至少 2 个核心交换机进行策略路由准入控制。
			准入设备可支持端口镜像准入技术，通过对交换机镜像数据的实时分析，能够及时发现并阻断非授权终端的接入。
			支持使用 802.1x MAC 认证时，记录详细的认证信息，包括:认证的时间、认证类型、认证的 MAC、认证是否成功等，并支持报表记录。
		定向引导	支持终端入网 IE 重定向引导，当用户访问网页时能够自动转向到指定的页面或地址，并支持 http 代理及多重重定向引导。
			可根据用户的实际环境自定义非 80 端口的 Web 服务端口号及用户重定向引导。
			能通过浏览器完成身份认证、控件安装、设备注册、安全检查、检查结果展现等全流程引导管理。
			▲具有 Mac OS、Linux、iOS、Android 等系统专属客户端，支持认证引导和准入管理（提供截图证明，加盖原厂商章）。
3	违规外联	▲违规外联	支持在终端上不安装任何客户端形式的软件支持终端违规外联行为功能（提供截图证明，加盖原厂商章）;
			能够针对 3G 拨号、双网卡、随身 WIFI、代理等多种违规联网行为做实时检测，不接受间歇性 ping 外网地址的探测方式。
			能够针对违规外联终端进行即时断网,断网方式应支持断开链接、关闭连接进程、断网后重启恢复、重启计算机等多级模式，并能够实时通知管理员。
			准入设备能够支持按照用户角色定义、限制员工的内网访问范围，防止其越权访问操作。
			SSID 白名单,可对连接到白名单之外的无线网络行为进行阻断(提供截图证明，加盖原厂商章)。
4	边界管理	IP/MAC 绑定	具有入网设备自动学习功能，支持 IP/MAC/端口三者强制绑定，以及违规终端 VLAN 隔离机制，防止终端仿冒 IP 接入网络或移动设备位置。
		主机防火墙	终端在准入通过后访问域严格收管理员策略控制
			同网段终端无法互相访问，做到精确到端口的高安全性控制
5	设备私接	NAT 设备	▲具有 NAT 识别和检测机制能够及时发现网内私接的小路由器、无线 AP、随身 WIFI 等 NAT 设备，帮助清查通过网中网隐藏的真

	管理		实网络终端（提供截图证明，加盖原厂商章）。
			对通过 NAT 入网的计算机可以实现准入控制、安全评估和修复等流程化管理提供截图证明，加盖原厂商章）。
		Hub 管理	能够发现内网私接的 Hub、傻瓜交换机等非网管设备，当多台计算机通过 Hub 接入网络时，能够及时产生告警通知管理员（提供截图证明，加盖原厂商章）。
			准入设备能够采用 VLAN 隔离、逻辑关闭端口等方式禁止 Hub 下联计算机接入网络。
			支持 Hub 下多个终端需分别认证才能入网和只需一台认证即可全部入网两种认证机制。
6	网络管理	设备识别	支持自动识别网络设备类型，包括：交换机、路由器、防火墙等，并按照类别自动进行归类。
			支持设备管理模板的定义功能，能够通过 SNMP、SSH、TELNET 等方式自动、批量添加网络设备。
		▲终端网络拓扑	准入设备支持交换机到终端计算机的网络拓扑管理功能，能够自动绘制出网络拓扑图（提供截图证明，加盖原厂商章）。
			能够在拓扑图上选取设备查看其基本状态信息、设备型号、所处位置、子节点、路由表、ARP 表等信息。
			支持在界面上提供对该网络设备进行 TELNET、SSH 等管理。
		交换机状态展现	支持可网管型交换机面板图形化展现各接口状态（up、down、trunk 等），以及各接口下联的终端详细信息（IP、地址、MAC 地址等）。
			能够支持自上而下逐级查找终端的具体位置、安全状态、认证用户、上下线时间等信息。
		AP 联动管理	能够与主流的 AP 设备深度联动，支持 AP 控制器面板的图形展现，包括 AP 连接状态、下联终端信息（IP 地址、MAC 地址等）等。
		DHCP 中继	能提供稳定的 DHCP 服务，并可以通过 DHCP 二次地址分配机制实现安全准入管理，支持交换机中继认证方式。
			能够根据用户、IP/MAC 绑定信息等条件，为指定终端设备分配特定的 IP 地址。
			支持 DHCP 服务器筛选，防止非法 DHCP 服务器分发错误地址
7	移动终端管理	终端识别	支持当前主流智能终端设备的安全准入控制，能够自动识别主流手机、智能终端等设备，并自动进行分类。
		移动终端入网	提供独立的智能终端入网引导界面的自主定制功能，至少包括界面标题、界面 LOGO、界面说明文字等。
			能够提供移动终端入网的设备注册功能。
8	认证管理	联动认证	能够全面结合用户已有的认证或业务系统，可以与 RADIUS、LDAP、STMP/POP 等采用标准协议的系统做深度联动认证。
		AD 域单点登录	能够与用户现有的 AD 域相结合，当用户登录到 AD 域后，无需二次认证即可入网，避免多次认证的繁琐流程。
			当用户未登录到 AD 域时，该终端将一直被隔离，该状态下只有通过 IE 页面进行认证才能够入网。

		证书认证	支持至少 2 个以上的根证书。终端用户认证时，自动进行认证证书的根证书匹配
		短信认证	支持短信认证模式，用户在登记入网手机号码后，能够在手机上接收到入网的短信验证码，并在 IE 页面上利用短信验证码认证入网。
		微信认证	通过关注微信公众号放行移动终端入网
		接入审核	能够针对不同的角色或设备类别有选择的开启入网审核功能，待审核的用户或设备必须经过管理员审批才能入网。
		认证控制	支持对认证时间段、IP 段控制限制某类（角色）账户只能在指定的时间段、IP 段认证。
		自助账号申请	支持用户在认证页面自行进行账号的申请。用户可自行提交用户名、密码、姓名、电话、部门、E-Mail 等信息。管理员审核通过后，用户即可使用该账号进行认证。有效解决用户账号和密码创建和分发的困难。
9	来宾管理	来宾角色	能够提供来宾角色选择，能够设定来宾设备的访问权限和入网时长
		来宾码认证	提供临时入网码，支持来宾设备与受访人员进行一对一绑定功能
		二维码认证	通过扫描二维码进行来宾入网管理
		来宾使用报表	生成来宾分配、来宾入网等动态审计报表
10	终端安全管理	安全检查库	准入设备提供系统安全配置、用户行为规范等类别检查项，至少提供 24 种以上安全检查项。
		系统补丁	▲准入设备具有完整的补丁管理子系统，无需第三方补丁服务器支持，自身可作为补丁服务器，自身即可以提供完整的流程化补丁管理，包括同步更新、补丁分类、补丁分发、补丁报表等功能（提供截图证明，加盖原厂商章）。
			能够在 IE 页面进行入网终端的补丁检查，补丁均划分为严重、重要、中等的类别，能够在 IE 页面显示出检查结果。
		防病毒软件	能够在 IE 页面检查出终端的杀毒软件情况，支持主流的 20 种以上的杀毒软件检查，包括微软 MSE、可牛、Avast 等，支持杀毒软件版本、病毒库和运行情况的检查，能够在 IE 页面显示出检查结果。
		Windows 组策略检测	windows 密码策略、屏保、共享目录、弱口令、防火墙、网卡配置等系统策略进行检查和修复
		计算机健康性检测	对终端的磁盘使用率、垃圾文件、IE 主页、网络监听端口等安全性配置进行检查和修复
		自定义安全检查	通过检测终端文件路径、指定文件版本、大小、MD5，注册表的项、注册表值，进程，服务名称、服务状态，进行检查。通过安装包运行、访问站点、开关服务、关闭进程、执行文件、删除文件、修改注册表进行修复。可以灵活的全访问的对终端进行安全检查和修复。

		终端安全加固	能够通过傻瓜式的漏洞修复模式为用户提供简单、形象的漏洞自我修复功能，完全不需要管理员的介入即可完成终端安全风险项修补。
		桌管系统联动	能够在 IE 页面检查出主流的桌面管理系统（包括 Landesk、北信源、威盾、盈高、圣博润等）客户端是否安装并正常运行，能够在 IE 页面显示出检查结果。
11	资源管理	软件检查	通过安全检查检测终端软件安装、使用状态
			自动强制为终端安装软件
			软件产品授权，支持进行 windows、office、WPS 的产品授权信息进行检查
		IP 地址管理	提供 IP 地址分配表，能够通过图示直观的查看各网段中未分配、开机、关机的数量和分布情况。
			能够直接、快捷的查看全网终端历史上线、下线、在线时长等详细的 IP 使用情况
		能耗管理	提供未关机终端自动统计功能，并能够按照部门、时间段等条件生成统计报表。
12	运维管理	移动终端管理	移动端管理平台可实现设备快速定位、设备审核、实时报警监控、小助手确认码生成、准入控制器管理、平台基本信息、关机与重启
		管理角色控制	准入设备须采用系统管理员、安全管理员、审计员三权分立机制，防止单个角色管理者权限滥用。
		网络诊断工具	支持通过 Web 管理界面提供 ping、抓包、traceroute、nslookup 等功能，并可以设置命令参数进行相关调试。
		消息群发	能够支持在指定的一台或者多台终端计算机上产生桌面消息通知，该消息会立即弹出在用户桌面上，对用户进行提醒。
		软件分发	准入设备应具有软件分发和部署功能，管理员可以预定义软件分发的路径、运行参数、是否执行等任务策略，以提升软件部署效率。
			能够自动判断并统计软件分发、部署的成功率，支持进程、注册表、安装路径等多种参数的组合判断。
13	报警报表管理	虚拟监控台	为了方便管理员从整体上把握网络安全态势，系统提供虚拟监控台功能。通过集中的仪表、数值显示快速进行安全态势的把握，主要包括：报警、安全风险等级、全网终端数、清理终端数、安检和规律、安检项状态分布。
		安全管理报表	准入设备后台能够按周、月、年统计安全状况走势图。
			准入设备后台提供每日入网报告、每周入网报告、每月入网报告。
		报警信息	可以提供紧急、重要、次要、提示等多个级别自定义报警模式。
			支持系统报警、网络报警、终端报警等类别，超过 20 种以上自定义报警类型。
			支持 Syslog 报警信息的定向输出。
		报警提醒	准入设备能够以邮件、手机短信、页面消息等多种报警方式提醒管理员各种安全异常状态。

14	▲第三方产品联动	支持与主流上网行为管理系统深度联动，构建内网准入、准出的全面安全管理体系。
		能够与主流动态口令认证系统相结合，提供动态密码联动认证机制。
		支持与国内外主流 U-Key 联动认证。
15	资质要求	公安部《计算机信息系统安全专用产品销售许可证-终端接入控制类》（提供证明文件，加盖原厂商章）
		国家保密局《涉密信息系统产品检测证书（网络访问控制产品）》（提供证明文件，加盖原厂商章）
		国家密码管理局《商用密码产品销售许可证》（提供证明文件，加盖原厂商章）
		中国信息安全认证中心《中国国家信息安全产品认证证书》（提供证明文件，加盖原厂商章）
16	▲保修	三年原厂硬件质保
17	▲其他	提供原厂商授权函及售后服务承诺函（加盖原厂商章）

（5）运维审计系统

序号	指标项	技术参数及技术要求
1	▲硬件指标	标准机架式设备，软硬一体化；单电源；10/100/1000M Base-TX 接口≥6个，存储容量≥1TB
		支持 700 路字符会话或 200 路图形会话并发
		包含 100 个点的被管资源数
		支持旁路部署
2	基础功能	将人与目标设备进行分离，建立以“人->用户账号->授权->目标设备账号->目标设备”为管理模式,通过基于唯一身份标识的集中管理账号与权限、授权的控制策略，与各服务器、网络设备等无缝连接，实现集中精细化运维操作管控与审计。
		支持协议：支持对运维操作（telnet/ssh/ftp/sftp/RDP/VNC/X11)的集中管理、访问控制、单点登录以及操作审计等功能。
		支持认证：系统提供身份认证，自然人（员工帐户）登录系统时支持静态口令、双因素认证、LDAP、AD 域。
		授权规则：系统提供用户对资源、用户组对资源组、用户组对资源、用户对资源组的灵活授权方式。
		账号代填：支持 Telnet、ssh、rdp、ftp/sftp 等协议的账号代填功能。
		支持审计功能：支持以 WEB 在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，支持离线回放重现维护人员对服务器的所有操作过程。可进行倍速/低速播放、拖动、暂停、停止、重新播放等播放控制操作。
		支持系统内置多种运行维护报表模板，支持以 CSV、HTML 方式生成并导出报表，支持管理员自定义审计报表，支持以日报、周报、月报的方式自动生成周期性报表。
3	身份及认证管理	支持账号分属组织的管理模式，能够实现更完善的分权管理和分权审计
		支持管理员、运维用户的静态口令、数字证书、动态口令、LDAP、AD 域、Radius 等认证方式
		支持系统管理员、运维管理员、设备账号管理员、会话审计员、管理审计

序号	指标项	技术参数及技术要求
		员等管理员角色
4	账号口令集中管理	支持对后台各类资源（主机、服务器、网络设备、数据库等）的账号口令进行统一管理，即后台资源的账号口令由系统托管，用户登录系统后，系统根据用户权限分配后台资源的使用权
5	SSO 单点登录	支持 Windows、Linux、Unix 等服务器账号自动登录
		支持 CISCO(包括特权账号)、H3C 等网络设备账号自动登录
		支持 FTP、VNC、SFTP 等账号自动登录
6	实时监控及阻断	监控正在运维的会话，信息包括运维用户、运维客户端地址、资源地址、协议、开始时间等
		提供在线运维操作的实时监控功能。针对命令协议和图形协议可以图像方式实时监控正在运维的各种操作，其信息与运维客户端所见完全一致
		管理员可以关闭在线会话
7	完整记录网络会话过程	系统提供运维协议 Telnet、FTP、SSH、SFTP、RDP（Windows Terminal）、Xwindows、VNC、Http、Https 以及应用发布等网络会话的完整会话记录
8	▲保修	三年原厂硬件质保

（6）数据审计系统

序号	指标项	指标参数
1	硬件指标	系统：审计产品采用专用工控机硬件架构，非普通 PC 服务器， MTBF(平均故障间隔时间)≥65000 小时；
		▲系统启动采用 CF 卡加硬盘方式，保证稳定可靠不可篡改（提供产品图片，加盖原厂商章）
		处理器：Intel E3 以上以上 CPU，至少 4 核 4 线程，主频至少 3.1G 以上；
		内存≥8GB；
		电源模块：具备冗余热插拔双电源；冗余热插拔风扇；
		硬盘可用容量≥2TB；支持 RAID1 阵列，最大支持扩展到 4T*2。
		网络端口：支持千兆网络环境下的监听能力，千兆业务电口≥4 个，千兆业务光口≥4 个，千兆 SFP 模块≥2 个；千兆管理电口≥2 个；
		审计性能：能够稳定、流畅地同时支持≥8 个数据库数审计能力，不会产生漏审；
2	部署方式	支持在目标数据库安装 agent 解决云环境、虚拟化环境内部流量无法镜像场景下数据库的审计（提供公安部三所或国家保密科技测评中心测评报告，加盖原厂商章）
		旁路部署模式下无须在被审计数据库系统上安装任何代理即可实现审计
		支持分布式部署，管理中心可实现统一配置、统一报表生成、统一查询；
		管理中心和探测器都可存储审计数据，实现大数据环境下磁盘空间的有效利用和扩展；
		管理中心和探测器直接的数据传输速率、时间、端口都可自定义（提供截图证明，加盖原厂商章）；
		▲支持大数据平台部署，具有成熟的大数据 hadoop 平台处理，支持后期无缝扩展大数据版本，支持审计数据外送至大数据平台，检索性能高达 100 亿数据仅需 6-8 秒，存储数据量高达 3000 亿以上，至少提供一个 100 万以上大数据处理合同案例（提供大数据合同关键页面复印件，加盖原厂商章）

3	处理能力	吞吐能力≥3000M；峰值处理能力≥3 万条/秒；日志数量存储≥5 亿条
		审计日志检索能力：≥1500 万条/秒；
4	协议支持	支持 Oracle、SQL-Server、DB2、Informix、Sybase、MySQL 等六种主流数据库审计；
		支持 PostgreSQL、Teradata、Cache、人大金仓、达梦、南大通用等数据库审计；
		支持主流业务协议 HTTP、Telnet、FTP、SMTP、POP3、DCOM；
		支持对各种协议自动识别编码及在 web 界面手工配置特定编码 （提供截图证明，加盖原厂商章）
5	审计功能	支持数据库操作类、表、视图、索引、存储过程等各种对象的所有 SQL 操作审计；
		支持对操作时间、SQL 语句、执行结果、影响行数、执行时长、数据库用户名，返回结果集、实例名、源/目的 IP、源/目的端口、源/目的 MAC、客户端主机名、客户端程序名称、客户端操作系统用户名、业务主机群、SQL 模板、会话 ID、事件唯一 ID 等至少 21 个条件进行审计；
		▲支持数据库请求和返回的双向审计，特别是返回字段和结果集、执行状态、返回行数、执行时长等内容，支持通过返回行数和内容大小控制返回结果集大小 （提供截图证明，加盖原厂商章；并提供公安部三所或国家保密科技测评中心检测报告，加盖原厂商章）；
		支持跨语句、跨多包的绑定变量名及绑定变量值的审计；
		支持导入审计关联的账号信息，支持通过 IP 和账号关联到具体 SQL 是哪个自然人操作；
		▲支持在 IPV6 环境中部署，且支持所有数据库 IPV6 协议的审计（提供截图证明，加盖原厂商章）；
6	智能发现	自动识别流量中存在的数据库，也可通过扫描发现网络中的数据库（提供截图证明，加盖原厂商章）；
		▲支持定期自动扫描数据库漏洞和不安全配置，提供漏洞扫描报告；（提供截图证明，加盖原厂商章；并提供公安部三所或国家保密科技测评中心检测报告，加盖原厂商章）；
7	应用关联 (三层关联)	▲支持 B/S 业务系统三层关联审计（提供截图证明，加盖原厂商章；并提供公安部三所或国家保密科技测评中心检测报告，加盖原厂商章）；
		支持 C/S、B/S 三层架构下的真实用户名关联配置；
		支持通过部署 agent 实现 java web 环境 100%准确关联（提供截图证明，加盖原厂商章）；
		支持旁路自动学习三层审计关联功能（提供截图证明，加盖原厂商章）；
8	运维审计	支持与堡垒主机自动关联审计通过 ssh、rdp 等加密协议操作数据库行为（提供截图证明，加盖原厂商章；并提供公安部三所或国家保密科技测评中心检测报告，加盖原厂商章）；
9	安全审计	支持审计记录中敏感数据的模糊化处理，内置常见敏感数据掩码规则，支持自定义敏感数据掩码规则（提供截图证明，加盖原厂商章）；
		内置安全特征库规则不少于 300 条，支持对数据库安全进行检查，如 SQL 注入，缓冲区溢出，数据库漏洞、弱口令等（提供截图证明，加盖原厂商章）；
10	审计策略	内置审计规则库不少于 200 条。支持事件类型和策略分组，同时支持黑白名单方式策略

		告警分析应支持根据 SQL 模板排行分析，便于告警处理。
		告警查询应支持根据登陆用户、客户端工具名、客户端 IP、规则进行归并分析，能详细展示每类告警占总告警数量百分比，便于告警分析处理（提供截图证明，加盖原厂商章）；
11	统计报表	系统提供内置多种报表模板库，内置的报表不少于 35 种（提供截图证明，加盖原厂商章）；
		支持根据单个数据库或逻辑数据库组生成报表(提供截图证明,加盖原厂商章)；
		报表支持严格按照塞班斯(SOX)法案、等级保护标准要求生成多维度综合报告；
		支持按照源 IP 地址、客户端工具、帐号、告警数等源信息生成报表；
		支持定期自动生成审计报表且以电子邮件方式自动进行发送（提供截图证明，加盖原厂商章）；
		支持报表自定义，自定义的条件不少于 20 个（提供截图证明，加盖原厂商章）；
12	模型分析	▲支持对数据库自动建模及智能对异常行为告警功能；（（提供截图证明，加盖原厂商章；并提供公安部三所或国家保密科技测评中心检测报告，加盖原厂商章）；
		可通过行为轨迹图方式展示数据库访问行为（提供截图证明，加盖原厂商章）；
		可基于账号、IP 地址、访问权限、客户端工具等维度对行为模型做钻取分析、变更分析，对学习的安全基线以外的行为自动智能的进行告警（提供截图证明，加盖原厂商章）；
		可以自动对比不同时期的行为模型，以区分其审计日志数趋势、用户、IP 地址、工具、访问权限的差异情况（提供截图证明，加盖原厂商章）；
		提供审计策略和系统配置信息的单独导入、导出功能；
13	实时监视	提供用户界面告警、Syslog 告警、SNMP 告警、邮件告警、短信告警、ftp 告警等六种方式
		支持本地和数据中心查看 CPU、内存、磁盘、网口、运行状态等信息
14	系统管理	采用 B/S 架构管理，支持中英文两种管理界面(提供截图证明，加盖原厂商章)；
		支持离线手工自动升级，升级数据和配置均需保留
		支持三权分立，系统默认设定系统管理员、规则配置员、审计查看员、操作日志查看员等角色
15	故障排错	系统内置独立的故障排错系统，可以支持一键导出加密的系统调试日志，支持一键检测服务、许可证、流量等大部分常见常见故障的检测（提供截图证明，加盖原厂商章）；
		支持流量分析功能，包括抓包、包内容查看、自动探测 sql 语句等（提供截图证明，加盖原厂商章）；
16	产品资质	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》，数据库安全审计国标-增强级；数据库审计产品专有的资质，不能是网络审计产品或者综合审计的产品资质（提供复印件，加盖原厂商章)；
		内置的数据库扫描系统通过国家相关部门的认证和检测，并获得独立的销售许可涉密资质；数据库审计产品专有的资质，不能是网络审计产品或者综合审计的产品资质（提供复印件，加盖原厂商章)；
17	厂家资质	厂商获得国家信息安全测评信息安全服务资质证书（安全工程类三级）（提供复印件，加盖原厂商章)；
18	▲保修	三年原厂硬件质保

19	▲其他	**提供原厂商授权函及售后服务承诺函（加盖原厂商章）**

（7）日志审计系统

序号	指标项	技术参数及技术要求
1	硬件要求	标准 2U 机架式硬件，软硬一体化设备；
		双电源；千兆审计口≥4 个,内存≥16GB；磁盘≥2T*2，raid1；
		日志解析处理能力≥8000EPS；网络流量≥800Mb；日志容量≥1.5 亿条；支持审计日志源≥100 个；
2	工作模式	▲为保障设备稳定运行，设备应支持 CF 卡启动（提供第三方检测报告复印件，并加盖原厂商章）；
		独立完成审计日志采集，不依赖于设备或系统自身的日志系统；
		审计工作不影响被审计对象的性能、稳定性或日常管理流程；
		审计结果存储于独立存储空间；
		自身用户管理与设备或主机的管理、使用、权限无关联；
		提供全中文 WEB 管理界面，无需安装任意客户端软件或插件；
3	功能扩展	▲采用解决方案包上传对产品进行功能扩展，无需要代码开发。
4	日志收集	支持 Syslog、SNMP Trap、OPSec、FTP 协议日志收集；
		支持使用代理(Agent)方式提取日志并收集；
		支持目前主流的网络安全设备、交换设备、路由设备、操作系统、应用系统等；
		支持设备厂家包括但不限于：Cisco(思科)，Juniper，联想网御/网御神州，F5，华为，H3C，微软，绿盟，飞塔(fortinet)，Foundry，天融信，启明星辰，天网，趋势，东软，Nokia，CheckPoint，Hillstone(山石)，安恒，珠海伟思，BEA，中国电信，安氏，帕拉迪，apc，arbor，clam，戴尔（dell），digium，东方电子，EMC，中国电力科学研究院，Eudora，google，冠群金辰，linksys，Mcafee，netapp，NAS（美国国家安全局），永达，sonicwall，vigor，天存，西岭，Symantec（赛门铁克），Hardened-PHP，foundertech(方正)，三零盛安，allot，蓝盾，IBM，金诺网安，网威，nortel(北电)，citrix(思杰)，watchguard，中兴，阿帕奇，WINDOWS 系统日志，Linux/UNIX syslog、IIS、Apache 等；
		支持常见的虚拟机环境日志收集，包括 Xen、VMWare、Hyper-V 等；
5	性能监控	▲能够通过在目标主机上安装 agent 程序，支持监测目标主机的 CPU 利用率、内存使用率、磁盘使用情况、流量等信息、监测结果正确并支持设置报警阈值（提供公安部计算机信息系统安全产品质量监督检验中心检验报告，加盖原厂商章）。
6	日志备份	可设置日志存储备份策略。包括系统日志保存期（天）、磁盘使用率百分比；支持日志备份自动传送到远程服务器；
7	日志分析	支持基于内存的实时关联分析，跨设备的多事件关联分析；（提供第三方检测报告复印件并加盖原厂商章）
		支持自定义条件的事件进行聚合；（提供截图并加盖原厂商章） 进行关联分析的规则可定制
		▲支持根据资产价值、资产漏洞、针对漏洞的威胁事件三者进行威胁的自动关联分析（三维关联），所有的三维关联算法和准则以 CVE、Bugtraq、OWASP 公开协议和标准为为基础。（提供第三方检测报告复印件并加盖原厂商章）
8	日志查询	支持 B/S 模式管理，支持 SSL 加密模式访问；

		支持按日期、时间、设备类型、日志类型、日志来源、威胁值、源地址、目的地址、事件类型、时间范围、操作对象、技术方式、技术动作、技术效果、攻击类型、地理城市等参数进行过滤查询；
		支持用任意关键字对所有事件进行高性能全文检索
		支持可指定多个查询条件进行组合查询
		支持将查询的条件存储为查询模版，方便再次使用
		极高的日志高查询性能，支持亿级的日志里根据做任意的关键字及其它的检索条件，在秒级里返回查询结果。
9	弱点管理	▲支持导入多个扫描器厂商的扫描报告，可进行统一检索、并支持计算威胁等级，范围 0~10（提供公安部计算机信息系统安全产品质量监督检验中心检验报告，加盖原厂商章）。
10	告警功能	可预设置安全告警策略； 支持数据阀值设置，超过阀值将产生告警
		可以通过邮件、短信和屏幕显示进行告警；支持自动防止报警信息在短时间内大量发送(告警抑制)；具备报警合并和在一个时间段内抑制报警次数的能力。
11	综合查询及报表管理	内置合规性报表 1000+种；
		内置 SOX、ISO27001、WEB 安全等解决方案包
		内置完善的等级保护合规报表（提供截图证明，加盖原厂商章）
		内置综合性自动化审计报告；支持用户自定义报表，自定义的报表支持多个统计维度的数据集合，支持报表导出为 PDF 和 Word 格式文件。
12	用户管理	根据三权分立的原则和要求进行职、权分离，对系统本身进行分角色定义，如管理员只负责完成设备的初始配置，规则配置员只负责审计规则的建立，审计员只负责查看相关的审计结果及告警内容；日志员只负责完成对系统本身的用户操作日志管理。
		系统自带自身管理日志
		▲注册用户资产时，提供自动发现识别能力。提供一键式故障排除功能。
		提供自助式的升级接口，支持对产品升级、规则升级（提供截图证明，加盖原厂商章）。
13	部署方式	支持分布式部署；支持集中式管理和升级模式；
		支持分级管理模式；
		采用 B/S 架构操作方式，无需客户端安装。
		支持监控设备自身 CPU、内存、磁盘等工作运行状况
14	产品资质	产品获得公安部计算机信息系统安全产品销售许可证以及公安部信息安全产品检测中心出具产品检验报告，所提供的产品检验报告须符合《信息安全技术日志分析产品检验规范》。提供证书及完整检测报告（行标三级）复印件，加盖原厂商章
		产品通过国家保密科技测评中心检测并获得涉密信息系统产品检测证书，符合《涉及国家秘密的信息系统安全监控与审计产品技术要求》。提供完整的检测报告复印件，加盖原厂商章
		产品获得中国信息安全认证中心颁发的《IT 产品信息安全认证证书》，检测标准符合 ISCCC-TR-056-2016《日志采集与分析产品安全技术要求》。提供完整的检测报告，加盖原厂商章
15	厂商资质要求	厂商获得知识产权管理体系认证证书（提供证书复印件，加盖原厂商章）
		厂商获得国家安全生产监督管理总局颁发的安全生产标准化三级企业证书；（提供证书复印件，加盖原厂商章）

16	▲保修	三年原厂硬件质保
17	▲其他	**提供原厂商授权函及售后服务承诺函（加盖原厂商章）**

（8）网络管理平台

序号	指标项	技术参数及技术要求
1	配置要求	配置网络管理系统一套，网元管理许可数量≥200
2	▲自动发现拓扑	支持自动搜索网络、发现网络节点，包括：网络设备、服务器、非网管设备的发现、PC 主机等，并基于网络的二层连接关系构建物理拓扑。自动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（提供软件页面截图和第三方检验报告复印件，加盖厂商项目授权章）
3	智能告警	通过实时的网络运行监测，系统可智能分析和预测潜在故障，并根据告警程度的不同发送警报。包括告警分类关联分析、告警多源关联分析、告警拓扑根源分析、告警网络影响度分析
4	▲网络拓扑管理	支持 IP 拓扑、二层拓扑、邻居拓扑、网络拓扑视图（支持网络区域的任意划分、命名、拖拽、折叠和展开）、业务拓扑、STP 拓扑、MSTP 拓扑等多种拓扑类型；二层拓扑支持多协议，包括 Bridge、NDP、CDP、MSTP、STP、LLDP、DISMAN-PING 等二层协议，支持聚合链路，支持第三方的设备；拓扑可融合链路状态、设备告警等多种信息（提供软件页面截图和第三方检验报告复印件，加盖厂商项目授权章）
		为了便于管理员编排展示页面，要求管理员可以首页中通过拖拽，自定义需要在首页展示页面（提供软件页面截图和第三方检验报告复印件，加盖厂商项目授权章）
5	权限管理	支持多用户，多角色，IT 运维人员，决策人员，不同角色有不同权限，不同区域级别也有不同权限。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
6	性能监控	支持从路由、设备、终端、流量、故障等方面多角度、细颗粒度地监控、管理整个 IT 网络。支持基于任务的性能监控，可定制监控任务，长期监控网络性能，可以形成日报、周报、月报等报表。支持定制性能阈值，可以为监控的性能指标设置两级阈值，当性能指标超过阈值时根据不同的阈值发送不同级别的告警
7	▲批量配置备份	对用户端交换机定期进行配置备份并支持配置检查工作，可根据配置模板自动进行配置比对，并以告警方式提供报告。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。（提供第三方检验报告复印件，加盖厂商项目授权章）
8	▲配置集中管理	支持设备配置集中管理：配置库包括配置文件和配置片断，配置内容可带有参数，在部署时根据设备的差异设置不同的值；配置文件可部署到设备的启动配置或者运行配置；配置片断只能部署到设备的运行配置。（提供第三方检验报告复印件，加盖厂商项目授权章）
9	多平台支持	支持 Windows、Linux 平台及 MS SQL、Oracle 数据库，支持 B/S 架构等主流平台
10	▲多厂商设备共同管理	支持管理第三方设备：新设备注册，告警注册，新性能指标注册，新 Syslog 解析注册，Mib 编译，第三方设备配置管理-CLI 下发，配置管理-配置备份，

序号	指标项	技术参数及技术要求
		支持多个厂商。（提供第三方检验报告复印件，加盖厂商项目授权章）
11	报表导出	可以直接打印或传真报表，也可以选择将报表导出。导出的格式包括 Microsoft Word（RTF）、Microsoft Excel、HTML、PDF、XML、CSV、TXT 等
12	分布式部署	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
13	▲业务联动控制	根据预定义的联动策略对匹配的事件（Trap）执行联动控制；支持各类安全威胁的分析和联动（支持防火墙、IPS、交换机、终端软件等上报信息的分析）；并支持在拓扑中显示攻击路径、攻击源等节点信息
14	▲保修	三年软件升级、原厂质保
15	▲其他	**提供原厂商授权函及售后服务承诺函（加盖原厂商章）**

（9）网络管理平台服务器

序号	指标项	技术参数及技术要求
1	处理器	单颗处理器核数≥6 核，主频≥1.6GHz，缓存≥15MB；本次配置处理器数量≥1
2	内存	≥24GB DDR4
3	硬盘	≥2*300GB 2.5 寸热插拔 SAS 硬盘
4	RAID 卡	支持 RAID 0/1，缓存≥2GB
5	网卡	≥4 个千兆电口
6	电源	1 个热插拔电源
7	其他	集成阵列卡(支持 Raid0/1)，DVD 光驱
8	保修	三年原厂硬件质保

2、视频专网

（1）边界防火墙

序号	指标项	技术参数及技术要求
1	▲基本配置	双冗余电源；≥6 个 10/100/1000M Base-TX 接口，≥4 个 SFP 接口；
		最大并发连接数≥320 万，最大吞吐量≥12Gbps，每秒新建连接数≥10 万；
		配置 IPS 模块，含三年特征库升级
2	网络适应性	支持静态路由，动态路由（OSPF、RIP 等），VLAN 间路由，组播路由等。
3	网络管理	支持 DHCP Client、DHCP Relay、DHCP Server。
		支持链路聚合功能，支持静态轮询、热备等多种模式。
		支持基于数据包的安全域、地址、用户及用户组、MAC、端口号、服务、域名等进行安全策略控制 。
		支持策略命中数显示。
		支持根据 IP 地址进行策略查询、支持根据服务端口进行策略查询。
4	入侵防护	支持基于策略的入侵检测与防护，可针对不同的源目 IP 地址、服务、用户等，采用不同的入侵防护策略。
		入侵防御特征库库包括信息窃取、木马后门、间谍软件、可疑行为、网络设备攻击、安全漏洞及网络数据库攻击等的特征事件。
		支持细粒度的自定义 IPS 特征功能。

		支持对网络扫描行为的检测和过滤，可实现基于端口的扫描防护和基于主机的扫描防护。
		支持 IP/MAC 地址绑定的方式防止 ARP 欺骗。
		支持丢弃封包、切断会话、攻击重定向、记录日志等响应方式。
		支持实时的入侵防护事件分级报警列表，可按事件的源 IP、目的 IP、协议、时间等显示。
5	统一认证管理	支持多人使用同一帐号登录。
		支持对 WEB 认证、LDAP 认证、RADIUS 认证。
		支持用户口令复杂度设置。
		支持显示详细的用户在线信息，包括用户名称、登录 IP/MAC、在线时间、登录时间等。
6	主动防御	支持 IPv4 和 IPv6 双栈协议下的主动防御。
7	安全日志	支持中文日志记录。
		支持对日志文件的导出/导入
8	高可用性	可在热备和集群工作模式下支持多台防火墙的会话、配置的实时同步、手动同步。
		支持基于 VRRP 技术的热备和负载均衡。
		在 NAT、路由、透明模式下支持 A-A,A-S 模式。
9	▲保修	三年原厂硬件质保

（2）终端准入控制系统

序号	指标项		技术参数及技术要求
1	基本要求	▲系统要求	具有独立自主知识产权，须为标准机架式硬件产品，除自身硬件设备外，产品功能的实现无需额外增加服务器等设备。配置设备指纹识别模块。
		▲硬件要求	采用标准机架式硬件设备，千兆电口≥6 个
		▲性能要求	每秒事务数（TPS）≥6000（次/秒），最大吞吐量≥2.3Gbps，最大并发链接数≥5000（条）；用户许可≥2500。
		高可用性	准入设备具备 HA 模式，HA 支持主备机心跳 IP 检测及虚地址管理模式，支持 vrrp 管理模式。
			提供第三方监控平台，在出现重大异常情况时能及时通知网络设备放开网络。
		终端部署	准入设备至少提供安全客户端（Agent）、安全控件、无客户端等多种可供自定义部署、管理模式。
			安全客户端模式部署时，客户端程序应支持功能定制，以降低系统资源耗用，提升客户端兼容性。
2	准入架构	终端发现	能够实时监测并发现接入内网的 PC、平板电脑、智能手机、IP 设备等终端，能够在第一时间隔离阻断并通知管理员。
			对自动发现的终端能够按照类别自动归类，以方便网络终端的统计管理（提供截图证明，加盖原厂商章）。
		准入技术	准入设备原生支持 802.1x 标准协议，无需第三方 RADIUS 服务器支

			持。
			▲准入设备支持基于多厂商 Virtual Gateway 的 VLAN 隔离技术，实现无客户端环境下端口级准入控制（提供截图证明，加盖原厂商章）。
			▲准入控制设备支持不少于 3 种准入技术，并可以提供同时使用（提供截图证明，加盖原厂商章）。
			准入设备支持基于策略路由技术的准入控制模式，入网设备在访问网内关键资源时，将被强制隔离、引导至认证管理页面，同时支持交换机接口动态 VLAN 下发、端口隔离模式的网络边界管理。
			单台准入设备可支持至少 2 个核心交换机进行策略路由准入控制。
			准入设备可支持端口镜像准入技术，通过对交换机镜像数据的实时分析，能够及时发现并阻断非授权终端的接入。
			支持使用 802.1x MAC 认证时，记录详细的认证信息，包括:认证的时间、认证类型、认证的 MAC、认证是否成功等，并支持报表记录。
		定向引导	支持终端入网 IE 重定向引导，当用户访问网页时能够自动转向到指定的页面或地址，并支持 http 代理及多重重定向引导。
			可根据用户的实际环境自定义非 80 端口的 Web 服务端口号及用户重定向引导。
			能通过浏览器完成身份认证、控件安装、设备注册、安全检查、检查结果展现等全流程引导管理。
			▲具有 Mac OS、Linux、iOS、Android 等系统专属客户端，支持认证引导和准入管理（提供截图证明，加盖原厂商章）。
3	违规外联	▲违规外联	支持在终端上不安装任何客户端形式的软件支持终端违规外联行为功能（提供截图证明，加盖原厂商章）;
			能够针对 3G 拨号、双网卡、随身 WIFI、代理等多种违规联网行为做实时检测，不接受间歇性 ping 外网地址的探测方式。
			能够针对违规外联终端进行即时断网，断网方式应支持断开链接、关闭连接进程、断网后重启恢复、重启计算机等多级模式，并能够实时通知管理员。
			准入设备能够支持按照用户角色定义、限制员工的内网访问范围，防止其越权访问操作。
			SSID 白名单，可对连接到白名单之外的无线网络行为进行阻断（提供截图证明，加盖原厂商章）。
4	边界管理	IP/MAC 绑定	具有入网设备自动学习功能，支持 IP/MAC/端口三者强制绑定，以及违规终端 VLAN 隔离机制，防止终端仿冒 IP 接入网络或移动设备位置。
		主机防火墙	终端在准入通过后访问域严格收管理员策略控制
			同网段终端无法互相访问，做到精确到端口的高安全性控制
5	设备私接管理	NAT 设备	▲具有 NAT 识别和检测机制能够及时发现网内私接的小路由器、无线 AP、随身 WIFI 等 NAT 设备，帮助清查通过网中网隐藏的真实网络终端（提供截图证明，加盖原厂商章）。
			对通过 NAT 入网的计算机可以实现准入控制、安全评估和修复等流程化管理提供截图证明，加盖原厂商章）。
		Hub 管理	能够发现内网私接的 Hub、傻瓜交换机等非网管设备，当多台计算

			机通过 Hub 接入网络时，能够及时产生告警通知管理员（提供截图证明，加盖原厂商章）。
			准入设备能够采用 VLAN 隔离、逻辑关闭端口等方式禁止 Hub 下联计算机接入网络。
			支持 Hub 下多个终端需分别认证才能入网和只需一台认证即可全部入网两种认证机制。
6	网络管理	设备识别	支持自动识别网络设备类型，包括：交换机、路由器、防火墙等，并按照类别自动进行归类。
			支持设备管理模板的定义功能，能够通过 SNMP、SSH、TELNET 等方式自动、批量添加网络设备。
		▲终端网络拓扑	准入设备支持交换机到终端计算机的网络拓扑管理功能，能够自动绘制出网络拓扑图（提供截图证明，加盖原厂商章）。
			能够在拓扑图上选取设备查看其基本状态信息、设备型号、所处位置、子节点、路由表、ARP 表等信息。
			支持在界面上提供对该网络设备进行 TELNET、SSH 等管理。
		交换机状态展现	支持可网管型交换机面板图形化展现各接口状态（up、down、trunk 等），以及各接口下联的终端详细信息（IP、地址、MAC 地址等）。
			能够支持自上而下逐级查找终端的具体位置、安全状态、认证用户、上下线时间等信息。
		AP 联动管理	能够与主流的 AP 设备深度联动，支持 AP 控制器面板的图形展现，包括 AP 连接状态、下联终端信息（IP 地址、MAC 地址等）等。
		DHCP 中继	能提供稳定的 DHCP 服务，并可以通过 DHCP 二次地址分配机制实现安全准入管理，支持交换机中继认证方式。
			能够根据用户、IP/MAC 绑定信息等条件，为指定终端设备分配特定的 IP 地址。
			支持 DHCP 服务器筛选，防止非法 DHCP 服务器分发错误地址
7	移动终端管理	终端识别	支持当前主流智能终端设备的安全准入控制，能够自动识别主流手机、智能终端等设备，并自动进行分类。
		移动终端入网	提供独立的智能终端入网引导界面的自主定制功能，至少包括界面标题、界面 LOGO、界面说明文字等。
			能够提供移动终端入网的设备注册功能。
8	认证管理	联动认证	能够全面结合用户已有的认证或业务系统，可以与 RADIUS、LDAP、STMP/POP 等采用标准协议的系统做深度联动认证。
		AD 域单点登录	能够与用户现有的 AD 域相结合，当用户登录到 AD 域后，无需二次认证即可入网，避免多次认证的繁琐流程。
			当用户未登录到 AD 域时，该终端将一直被隔离，该状态下只有通过 IE 页面进行认证才能够入网。
		证书认证	支持至少 2 个以上的根证书。终端用户认证时，自动进行认证证书的根证书匹配

		短信认证	支持短信认证模式，用户在登记入网手机号码后，能够在手机上接收到入网的短信验证码，并在 IE 页面上利用短信验证码认证入网。
		微信认证	通过关注微信公众号放行移动终端入网
		接入审核	能够针对不同的角色或设备类别有选择的开启入网审核功能，待审核的用户或设备必须经过管理员审批才能入网。
		认证控制	支持对认证时间段、IP 段控制限制某类（角色）账户只能在指定的时间段、IP 段认证。
		自助账号申请	支持用户在认证页面自行进行账号的申请。用户可自行提交用户名、密码、姓名、电话、部门、E-Mail 等信息。管理员审核通过后，用户即可使用该账号进行认证。有效解决用户账号和密码创建和分发的困难。
9	来宾管理	来宾角色	能够提供来宾角色选择，能够设定来宾设备的访问权限和入网时长
		来宾码认证	提供临时入网码，支持来宾设备与受访人员进行一对一绑定功能
		二维码认证	通过扫描二维码进行来宾入网管理
		来宾使用报表	生成来宾分配、来宾入网等动态审计报表
10	终端安全管理	安全检查库	准入设备提供系统安全配置、用户行为规范等类别检查项，至少提供 24 种以上安全检查项。
		系统补丁	▲准入设备具有完整的补丁管理子系统，无需第三方补丁服务器支持，自身可作为补丁服务器，自身即可以提供完整的流程化补丁管理，包括同步更新、补丁分类、补丁分发、补丁报表等功能（提供截图证明，加盖原厂商章）。
			能够在 IE 页面进行入网终端的补丁检查，补丁均划分为严重、重要、中等的类别，能够在 IE 页面显示出检查结果。
		防病毒软件	能够在 IE 页面检查出终端的杀毒软件情况，支持主流的 20 种以上的杀毒软件检查，包括微软 MSE、可牛、Avast 等，支持杀毒软件版本、病毒库和运行情况的检查，能够在 IE 页面显示出检查结果。
		Windows 组策略检测	windows 密码策略、屏保、共享目录、弱口令、防火墙、网卡配置等系统策略进行检查和修复
		计算机健康性检测	对终端的磁盘使用率、垃圾文件、IE 主页、网络监听端口等安全性配置进行检查和修复
		自定义安全检查	通过检测终端文件路径、指定文件版本、大小、MD5，注册表的项、注册表值，进程，服务名称、服务状态，进行检查。通过安装包运行、访问站点、开关服务、关闭进程、执行文件、删除文件、修改注册表进行修复。可以灵活的全访问的对终端进行安全检查和修复。
		终端安全加固	能够通过傻瓜式的漏洞修复模式为用户提供简单、形象的漏洞自我修复功能，完全不需要管理员的介入即可完成终端安全风险项修补。
		桌管系统联动	能够在 IE 页面检查出主流的桌面管理系统（包括 Landesk、北信源、威盾、盈高、圣博润等）客户端是否安装并正常运行，能够在 IE

			页面显示出检查结果。
11	资源管理	软件检查	通过安全检查检测终端软件安装、使用状态
			自动强制为终端安装软件
			软件产品授权，支持进行 windows、office、WPS 的产品授权信息进行检查
		IP 地址管理	提供 IP 地址分配表，能够通过图示直观的查看各网段中未分配、开机、关机的数量和分布情况。
			能够直接、快捷的查看全网终端历史上线、下线、在线时长等详细的 IP 使用情况
		能耗管理	提供未关机终端自动统计功能，并能够按照部门、时间段等条件生成统计报表。
12	运维管理	移动终端管理	移动端管理平台可实现设备快速定位、设备审核、实时报警监控、小助手确认码生成、准入控制器管理、平台基本信息、关机与重启
		管理角色控制	准入设备须采用系统管理员、安全管理员、审计员三权分立机制，防止单个角色管理者权限滥用。
		网络诊断工具	支持通过 Web 管理界面提供 ping、抓包、traceroute、nslookup 等功能，并可以设置命令参数进行相关调试。
		消息群发	能够支持在指定的一台或者多台终端计算机上产生桌面消息通知，该消息会立即弹出在用户桌面上，对用户进行提醒。
		软件分发	准入设备应具有软件分发和部署功能，管理员可以预定义软件分发的路径、运行参数、是否执行等任务策略，以提升软件部署效率。
			能够自动判断并统计软件分发、部署的成功率，支持进程、注册表、安装路径等多种参数的组合判断。
13	报警报表管理	虚拟监控台	为了方便管理员从整体上把握网络安全态势，系统提供虚拟监控台功能。通过集中的仪表、数值显示快速进行安全态势的把握，主要包括：报警、安全风险等级、全网终端数、清理终端数、安检和规律、安检项状态分布。
		安全管理报表	准入设备后台能够按周、月、年统计安全状况走势图。
			准入设备后台提供每日入网报告、每周入网报告、每月入网报告。
		报警信息	可以提供紧急、重要、次要、提示等多个级别自定义报警模式。
			支持系统报警、网络报警、终端报警等类别，超过 20 种以上自定义报警类型。
			支持 Syslog 报警信息的定向输出。
		报警提醒	准入设备能够以邮件、手机短信、页面消息等多种报警方式提醒管理员各种安全异常状态。
14	▲第三方产品联动		支持与主流上网行为管理系统深度联动，构建内网准入、准出的全面安全管理体系。
			能够与主流动态口令认证系统相结合，提供动态密码联动认证机制。

		支持与国内外主流 U-Key 联动认证。
15	资质要求	公安部《计算机信息系统安全专用产品销售许可证-终端接入控制类》（提供证明文件，加盖原厂商章）
		国家保密局《涉密信息系统产品检测证书（网络访问控制产品）》（提供证明文件，加盖原厂商章）
		国家密码管理局《商用密码产品销售许可证》（提供证明文件，加盖原厂商章）
		中国信息安全认证中心《中国国家信息安全产品认证证书》（提供证明文件，加盖原厂商章）
16	▲保修	三年原厂硬件质保
17	▲其他	**提供原厂商授权函及售后服务承诺函（加盖原厂商章）**

（3）运维审计系统

序号	指标项	技术参数及技术要求
1	▲硬件指标	标准机架式设备，软硬一体化；单电源；10/100/1000M Base-TX 接口≥6个，存储容量≥1TB
		支持 700 路字符会话或 200 路图形会话并发
		包含 100 个点的被管资源数
		支持旁路部署
2	基础功能	将人与目标设备进行分离，建立以“人->用户账号->授权->目标设备账号->目标设备”为管理模式，通过基于唯一身份标识的集中管理账号与权限、授权的控制策略，与各服务器、网络设备等无缝连接，实现集中精细化运维操作管控与审计。
		支持协议：支持对运维操作（telnet/ssh/ftp/sftp/RDP/VNC/X11)的集中管理、访问控制、单点登录以及操作审计等功能。
		支持认证：系统提供身份认证，自然人（员工帐户）登录系统时支持静态口令、双因素认证、LDAP、AD 域。
		授权规则：系统提供用户对资源、用户组对资源组、用户组对资源、用户对资源组的灵活授权方式。
		账号代填：支持 Telnet、ssh、rdp、ftp/sftp 等协议的账号代填功能。
		支持审计功能：支持以 WEB 在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，支持离线回放重现维护人员对服务器的所有操作过程。可进行倍速/低速播放、拖动、暂停、停止、重新播放等播放控制操作。
		支持系统内置多种运行维护报表模板，支持以 CSV、HTML 方式生成并导出报表，支持管理员自定义审计报表，支持以日报、周报、月报的方式自动生成周期性报表。
3	身份及认证管理	支持账号分属组织的管理模式，能够实现更完善的分权管理和分权审计
		支持管理员、运维用户的静态口令、数字证书、动态口令、LDAP、AD 域、Radius 等认证方式
		支持系统管理员、运维管理员、设备账号管理员、会话审计员、管理审计员等管理员角色
4	账号口令集中管理	支持对后台各类资源（主机、服务器、网络设备、数据库等）的账号口令进行统一管理，即后台资源的账号口令由系统托管，用户登录系统后，系统根据用户权限分配后台资源的使用权

序号	指标项	技术参数及技术要求
5	SSO 单点登录	支持 Windows、Linux、Unix 等服务器账号自动登录
		支持 CISCO(包括特权账号)、H3C 等网络设备账号自动登录
		支持 FTP、VNC、SFTP 等账号自动登录
6	实时监控及阻断	监控正在运维的会话，信息包括运维用户、运维客户端地址、资源地址、协议、开始时间等
		提供在线运维操作的实时监控功能。针对命令协议和图形协议可以图像方式实时监控正在运维的各种操作，其信息与运维客户端所见完全一致
		管理员可以关闭在线会话
7	完整记录网络会话过程	系统提供运维协议 Telnet、FTP、SSH、SFTP、RDP（Windows Terminal）、Xwindows、VNC、Http、Https 以及应用发布等网络会话的完整会话记录
8	▲保修	三年原厂硬件质保

4、日志审计系统

序号	指标项	技术参数及技术要求
1	硬件要求	标准 2U 机架式硬件，软硬一体化设备；
		双电源；千兆审计口≥4 个,内存≥16GB；磁盘≥2T*2，raid1；
		日志解析处理能力≥8000EPS；网络流量≥800Mb；日志容量≥1.5 亿条；支持审计日志源≥100 个；
2	工作模式	▲为保障设备稳定运行，设备应支持 CF 卡启动（提供第三方检测报告复印件，并加盖原厂商章）；
		独立完成审计日志采集，不依赖于设备或系统自身的日志系统；
		审计工作不影响被审计对象的性能、稳定性或日常管理流程；
		审计结果存储于独立存储空间；
		自身用户管理与设备或主机的管理、使用、权限无关联；
		提供全中文 WEB 管理界面，无需安装任意客户端软件或插件；
3	功能扩展	▲采用解决方案包上传对产品进行功能扩展，无需要代码开发。
4	日志收集	支持 Syslog、SNMP Trap、OPSec、FTP 协议日志收集；
		支持使用代理(Agent)方式提取日志并收集；
		支持目前主流的网络安全设备、交换设备、路由设备、操作系统、应用系统等；
		支持设备厂家包括但不限于：Cisco(思科)，Juniper，联想网御/网御神州，F5，华为，H3C，微软，绿盟，飞塔(fortinet)，Foundry，天融信，启明星辰，天网，趋势，东软，Nokia，CheckPoint，Hillstone(山石)，安恒，珠海伟思，BEA，中国电信，安氏，帕拉迪，apc，arbor，clam，戴尔（dell），digium，东方电子，EMC，中国电力科学研究院，Eudora，google，冠群金辰，linksys，Mcafee，netapp，NAS（美国国家安全局），永达，sonicwall，vigor，天存，西岭，Symantec（赛门铁克），Hardened-PHP，foundertech(方正)，三零盛安，allot，蓝盾，IBM，金诺网安，网威，nortel(北电)，citrix(思杰)，watchguard，中兴，阿帕奇，WINDOWS 系统日志，Linux/UNIX syslog、IIS、Apache 等；
		支持常见的虚拟机环境日志收集，包括 Xen、VMWare、Hyper-V 等；

5	性能监控	▲能够通过在目标主机上安装 agent 程序,支持监测目标主机的 CPU 利用率、内存使用率、磁盘使用情况、流量等信息、监测结果正确并支持设置报警阈值（提供公安部计算机信息系统安全产品质量监督检验中心检验报告，加盖原厂商章）。
6	日志备份	可设置日志存储备份策略。包括系统日志保存期（天）、磁盘使用率百分比；支持日志备份自动传送到远程服务器；
7	日志分析	支持基于内存的实时关联分析，跨设备的多事件关联分析；（提供第三方检测报告复印件并加盖原厂商章）
		支持自定义条件的事件进行聚合；（提供截图并加盖原厂商章） 进行关联分析的规则可定制
		▲支持根据资产价值、资产漏洞、针对漏洞的威胁事件三者进行威胁的自动关联分析（三维关联），所有的三维关联算法和准则以 CVE、Bugtraq、OWASP 公开协议和标准为为基础。（提供第三方检测报告复印件并加盖原厂商章）
8	日志查询	支持 B/S 模式管理，支持 SSL 加密模式访问；
		支持按日期、时间、设备类型、日志类型、日志来源、威胁值、源地址、目的地址、事件类型、时间范围、操作对象、技术方式、技术动作、技术效果、攻击类型、地理城市等参数进行过滤查询；
		支持用任意关键字对所有事件进行高性能全文检索
		支持可指定多个查询条件进行组合查询
		支持将查询的条件存储为查询模版，方便再次使用
		极高的日志高查询性能，支持亿级的日志里根据做任意的关键字及其它的检索条件，在秒级里返回查询结果。
9	弱点管理	▲支持导入多个扫描器厂商的扫描报告，可进行统一检索、并支持计算威胁等级，范围 0~10（提供公安部计算机信息系统安全产品质量监督检验中心检验报告，加盖原厂商章）。
10	告警功能	可预设置安全告警策略； 支持数据阀值设置，超过阀值将产生告警
		可以通过邮件、短信和屏幕显示进行告警；支持自动防止报警信息在短时间内大量发送(告警抑制)；具备报警合并和在一个时间段内抑制报警次数的能力。
11	综合查询及报表管理	内置合规性报表 1000+种；
		内置 SOX、ISO27001、WEB 安全等解决方案包
		内置完善的等级保护合规报表（提供截图证明，加盖原厂商章）
		内置综合性自动化审计报告；支持用户自定义报表，自定义的报表支持多个统计维度的数据集合，支持报表导出为 PDF 和 Word 格式文件。
12	用户管理	根据三权分立的原则和要求进行职、权分离，对系统本身进行分角色定义，如管理员只负责完成设备的初始配置，规则配置员只负责审计规则的建立，审计员只负责查看相关的审计结果及告警内容；日志员只负责完成对系统本身的用户操作日志管理。
		系统自带自身管理日志
		▲注册用户资产时，提供自动发现识别能力。提供一键式故障排除功能。
		提供自助式的升级接口，支持对产品升级、规则升级（提供截图证明，加盖原厂商章）。
13	部署方式	支持分布式部署；支持集中式管理和升级模式；
		支持分级管理模式；
		采用 B/S 架构操作方式，无需客户端安装。

		支持监控设备自身 CPU、内存、磁盘等工作运行状况
14	产品资质	产品获得公安部计算机信息系统安全产品销售许可证以及公安部信息安全产品检测中心出具产品检验报告，所提供的产品检验报告须符合《信息安全技术日志分析产品检验规范》。提供证书及完整检测报告（行标三级）复印件，加盖原厂商章
		产品通过国家保密科技测评中心检测并获得涉密信息系统产品检测证书，符合《涉及国家秘密的信息系统安全监控与审计产品技术要求》。提供完整的检测报告复印件，加盖原厂商章
		产品获得中国信息安全认证中心颁发的《IT 产品信息安全认证证书》，检测标准符合 ISCCC-TR-056-2016《日志采集与分析产品安全技术要求》。提供完整的检测报告，加盖原厂商章
15	厂商资质要求	厂商获得知识产权管理体系认证证书（提供证书复印件，加盖原厂商章）
		厂商获得国家安全生产监督管理总局颁发的安全生产标准化三级企业证书；（提供证书复印件，加盖原厂商章）
16	▲保修	三年原厂硬件质保
17	▲其他	**提供原厂商授权函及售后服务承诺函（加盖原厂商章）**

（5）网络管理平台

序号	指标项	技术参数及技术要求
1	配置要求	配置网络管理系统一套，网元管理许可数量≥200
2	▲自动发现拓扑	支持自动搜索网络、发现网络节点，包括：网络设备、服务器、非网管设备的发现、PC 主机等，并基于网络的二层连接关系构建物理拓扑。自动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（提供软件页面截图和第三方检验报告复印件，加盖厂商项目授权章）
3	智能告警	通过实时的网络运行监测，系统可智能分析和预测潜在故障，并根据告警程度的不同发送警报。包括告警分类关联分析、告警多源关联分析、告警拓扑根源分析、告警网络影响度分析
4	▲网络拓扑管理	支持 IP 拓扑、二层拓扑、邻居拓扑、网络拓扑视图（支持网络区域的任意划分、命名、拖拽、折叠和展开）、业务拓扑、STP 拓扑、MSTP 拓扑等多种拓扑类型；二层拓扑支持多协议，包括 Bridge、NDP、CDP、MSTP、STP、LLDP、DISMAN-PING 等二层协议，支持聚合链路，支持第三方的设备；拓扑可融合链路状态、设备告警等多种信息（提供软件页面截图和第三方检验报告复印件，加盖厂商项目授权章）
		为了便于管理员编排展示页面，要求管理员可以首页中通过拖拽，自定义需要在首页展示页面（提供软件页面截图和第三方检验报告复印件，加盖厂商项目授权章）
5	权限管理	支持多用户，多角色，IT 运维人员，决策人员，不同角色有不同权限，不同区域级别也有不同权限。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
6	性能监控	支持从路由、设备、终端、流量、故障等方面多角度、细颗粒度地监控、管理整个 IT 网络。支持基于任务的性能监控，可定制监控任务，长期监控网络性能，可以形成日报、周报、月报等报表。支持定制性能阈值，可以

序号	指标项	技术参数及技术要求
		为监控的性能指标设置两级阈值，当性能指标超过阈值时根据不同的阈值发送不同级别的告警
7	▲批量配置备份	对用户端交换机定期进行配置备份并支持配置检查工作，可根据配置模板自动进行配置比对，并以告警方式提供报告。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。（提供第三方检验报告复印件，加盖厂商项目授权章）
8	▲配置集中管理	支持设备配置集中管理：配置库包括配置文件和配置片断，配置内容可带有参数，在部署时根据设备的差异设置不同的值；配置文件可部署到设备的启动配置或者运行配置；配置片断只能部署到设备的运行配置。（提供第三方检验报告复印件，加盖厂商项目授权章）
9	多平台支持	支持 Windows、Linux 平台及 MS SQL、Oracle 数据库，支持 B/S 架构等主流平台
10	▲多厂商设备共同管理	支持管理第三方设备：新设备注册，告警注册，新性能指标注册，新 Syslog 解析注册，Mib 编译，第三方设备配置管理-CLI 下发，配置管理-配置备份，支持多个厂商。（提供第三方检验报告复印件，加盖厂商项目授权章）
11	报表导出	可以直接打印或传真报表，也可以选择将报表导出。导出的格式包括 Microsoft Word（RTF）、Microsoft Excel、HTML、PDF、XML、CSV、TXT 等
12	分布式部署	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
13	▲业务联动控制	根据预定义的联动策略对匹配的事件（Trap）执行联动控制；支持各类安全威胁的分析和联动（支持防火墙、IPS、交换机、终端软件等上报信息的分析）；并支持在拓扑中显示攻击路径、攻击源等节点信息
14	▲保修	三年软件升级、原厂质保
15	▲其他	**提供原厂商授权函及售后服务承诺函（加盖原厂商章）**

（6）网络管理平台服务器

序号	指标项	技术参数及技术要求
1	处理器	单颗处理器核数≥6 核，主频≥1.6GHz，缓存≥15MB；本次配置处理器数量≥1
2	内存	≥24GB DDR4
3	硬盘	≥2*300GB 2.5 寸热插拔 SAS 硬盘
4	RAID 卡	支持 RAID 0/1，缓存≥2GB
5	网卡	≥4 个千兆电口
6	电源	1 个热插拔电源
7	其他	集成阵列卡(支持 Raid0/1)，DVD 光驱
8	保修	三年原厂硬件质保

（7）服务器接入交换机

序号	指标项	技术参数及技术要求
1	基本配置	10/100/1000Base-T 以太网端口≥48 个，其中 4 个复用的 1000Base-X 千兆 SFP 端口

序号	指标项	技术参数及技术要求
2	性能	交换容量≥200Gbps，包转发率≥90Mpps
3	IP 路由	支持静态路由，支持 RIPv1/v2，支持 OSPFv1/v2
4	管理与维护	支持命令行接口（CLI）、Telnet、Console 口进行配置，支持 SNMPv1/v2/v3
5	保修	三年原厂硬件质保

3、互联网

（1）边界防火墙

序号	指标项	技术参数及技术要求
1	▲基本配置	双冗余电源；≥4 个 10/100/1000M Base-TX 接口，≥2 个 SFP 接口；
		最大并发连接数≥300 万，最大吞吐量≥8Gbps，每秒新建连接数≥6 万；
		配置 IPS 模块、AV 模块，含三年特征库升级
2	网络适应性	支持静态路由，动态路由（OSPF、RIP 等），VLAN 间路由，组播路由等。
3	网络管理	支持 DHCP Client、DHCP Relay、DHCP Server。
		支持链路聚合功能，支持静态轮询、热备等多种模式。
		支持基于数据包的安全域、地址、用户及用户组、MAC、端口号、服务、域名等进行安全策略控制 。
		支持策略命中数显示。
		支持根据 IP 地址进行策略查询、支持根据服务端口进行策略查询。
4	入侵防护	支持基于策略的入侵检测与防护，可针对不同的源目 IP 地址、服务、用户等，采用不同的入侵防护策略。
		入侵防御特征库库包括信息窃取、木马后门、间谍软件、可疑行为、网络设备攻击、安全漏洞及网络数据库攻击等的特征事件。
		支持细粒度的自定义 IPS 特征功能，支持 DNS\HTTP\FTP\TFTP\TELNET\SNMP\POP3\SMTP\IMAP\等应用层协议的自定义。
		支持对网络扫描行为的检测和过滤，可实现基于端口的扫描防护和基于主机的扫描防护。
		支持 IP/MAC 地址绑定的方式防止 ARP 欺骗。
		支持丢弃封包、切断会话、攻击重定向、记录日志等响应方式。
		支持实时的入侵防护事件分级报警列表，可按事件的源 IP、目的 IP、协议、时间等显示。
5	恶意代码防护	支持基于策略的病毒扫描与防护，可针对不同的源目 IP 地址、源 MAC 地址、服务等，采用不同的病毒防护策略。
		支持应用协议自识别，可以实现 HTTP,SMTP,FTP,POP3,IMAP,FTP,WEBMAIL 多种应用协议下的病毒防护，支持自定义非标准端口下应用协议的病毒防护。
		支持常见 WEB 邮件系统的病毒防护。
		支持路由、透明、混合等各种工作模式下的网络病毒检测。
		支持隔离病毒源地址，防止病毒源主机访问内部网络，提高网络整体安全性。
		系统内置多种病毒防护模板，支持自定义病毒防护模板。
		支持过滤邮件病毒、文件病毒、恶意网页代码、木马后门、蠕虫等多种类

		型的病毒。
6	统一认证管理	支持多人使用同一帐号登录。
		支持对 WEB 认证、LDAP 认证、RADIUS 认证。
		支持用户口令复杂度设置。
		支持显示详细的用户在线信息，包括用户名称、登录 IP/MAC、在线时间、登录时间等。
7	主动防御	支持 IPv4 和 IPv6 双栈协议下的主动防御。
8	安全日志	支持中文日志记录。
		支持对日志文件的导出/导入
9	高可用性	可在热备和集群工作模式下支持多台防火墙的会话、配置的实时同步、手动同步。
		支持基于 VRRP 技术的热备和负载均衡。
		在 NAT、路由、透明模式下支持 A-A,A-S 模式。
10	▲保修	三年原厂硬件质保

（2）、边界 WEB 防火墙

序号	指标项	技术参数及技术要求
1	基本参数	10/100/1000 Base-T 接口（支持 bypass）≥4 个，应用吞吐量≥1G；
2	防护功能要求	支持 HTTP 0.9/1.0/1.1。
		支持扫描防护。
		支持 SQL 注入、XSS 防护，支持使 HTTP 头域中的 Cookie、Referer、User-Agent，Except 字段过防护策略。
		支持 CSRF（跨站请求伪造）防护。
		支持防护：蠕虫、缓冲区溢出、CGI 信息扫描、目录遍历等攻击。
		支持 Cookie 安全机制，包括加密和签名的防护方法，支持 Cookie 自学习。
		支持对服务器状态码进行过滤和伪装的安全策略。
		可以根据文件大小、MIME 类型、及文件扩展名，灵活定义下载限制策略，限制用户非法获取网站的关键数据（比如数据库文件，配置文件等）。
		支持 100 种以上爬虫防护；支持盗链防护，可采用 Referer 和 Cookie 算法。
		支持自动监测页面被篡改情况的功能，支持视觉恢复功能，即发生网页篡改后，对外仍显示被篡改前的正常页面，支持时间管理功能，可以在不同的时间段设定不同的网页篡改防护策略，支持恶意代码过滤功能，支持敏感关键字自定义功能。
		支持各类 DDOS 防护，包括 TCP Flood、HTTP Flood 防护，并说明 HTTP Flood 防护的检测算法。
		支持 HTTP 协议解码并对相关字段进行检查，包括 URI、HTTP 版本、请求方法、响应状态码、HTTP 头部各字段和其他 HTTP 元素。
		防护策略模型由基于静态规则的反向（黑名单）安全模式及基于智能用户行为识别的动态防护机制（正向安全模式，即白名单）构建。
		支持对 SSL（HTTPS）加密会话进行分析。

3	管理功能要求	支持标准 SNMP trap 和 Syslog 接口；支持 WEB 界面管理及 Console 及 SSH 管理。
		系统各组件通过强加密的 SSL 安全通道进行通讯，防止窃听，确保了整个系统的安全性和抗毁性；能对账户进行安全策略配置，包括口令最小长度和口令生存期；可以限制远程管理的登录 IP。
4	▲保修	三年原厂硬件质保
5	▲其他	**提供原厂商授权函及售后服务承诺函（加盖原厂商章）**

（3）终端准入控制系统

序号	指标项		技术参数及技术要求
1	基本要求	▲系统要求	具有独立自主知识产权，须为标准机架式硬件产品，除自身硬件设备外，产品功能的实现无需额外增加服务器等设备。配置设备指纹识别模块。
		▲硬件要求	采用标准机架式硬件设备，千兆电口≥6 个
		▲性能要求	每秒事务数（TPS）≥1500（次/秒），最大吞吐量≥800Mbps，最大并发链接数≥1600（条）；用户许可≥800。
		高可用性	准入设备具备 HA 模式，HA 支持主备机心跳 IP 检测及虚地址管理模式，支持 vrrp 管理模式。
			提供第三方监控平台，在出现重大异常情况时能及时通知网络设备放开网络。
		终端部署	准入设备至少提供安全客户端（Agent）、安全控件、无客户端等多种可供自定义部署、管理模式。
			安全客户端模式部署时，客户端程序应支持功能定制，以降低系统资源耗用，提升客户端兼容性。
2	准入架构	终端发现	能够实时监测并发现接入内网的 PC、平板电脑、智能手机、IP 设备等终端，能够在第一时间隔离阻断并通知管理员。
			对自动发现的终端能够按照类别自动归类，以方便网络终端的统计管理（提供截图证明，加盖原厂商章）。
		准入技术	准入设备原生支持 802.1x 标准协议，无需第三方 RADIUS 服务器支持。
			▲准入设备支持基于多厂商 Virtual Gateway 的 VLAN 隔离技术，实现无客户端环境下端口级准入控制（提供截图证明，加盖原厂商章）。
			▲准入控制设备支持不少于 3 种准入技术，并可以提供同时使用（提供截图证明，加盖原厂商章）。
			准入设备支持基于策略路由技术的准入控制模式，入网设备在访问网内关键资源时，将被强制隔离、引导至认证管理页面，同时支持交换机接口动态 VLAN 下发、端口隔离模式的网络边界管理。
			单台准入设备可支持至少 2 个核心交换机进行策略路由准入控制。
			准入设备可支持端口镜像准入技术，通过对交换机镜像数据的实时分析，能够及时发现并阻断非授权终端的接入。

			支持使用 802.1x MAC 认证时，记录详细的认证信息，包括:认证的时间、认证类型、认证的 MAC、认证是否成功等，并支持报表记录。
		定向引导	支持终端入网 IE 重定向引导，当用户访问网页时能够自动转向到指定的页面或地址，并支持 http 代理及多重重定向引导。
			可根据用户的实际环境自定义非 80 端口的 Web 服务端口号及用户重定向引导。
			能通过浏览器完成身份认证、控件安装、设备注册、安全检查、检查结果展现等全流程引导管理。
			▲具有 Mac OS、Linux、iOS、Android 等系统专属客户端，支持认证引导和准入管理（提供截图证明，加盖原厂商章）。
3	违规外联	▲违规外联	支持在终端上不安装任何客户端形式的软件支持终端违规外联行为功能（提供截图证明，加盖原厂商章）;
			能够针对 3G 拨号、双网卡、随身 WIFI、代理等多种违规联网行为做实时检测，不接受间歇性 ping 外网地址的探测方式。
			能够针对违规外联终端进行即时断网，断网方式应支持断开链接、关闭连接进程、断网后重启恢复、重启计算机等多级模式，并能够实时通知管理员。
			准入设备能够支持按照用户角色定义、限制员工的内网访问范围，防止其越权访问操作。
			SSID 白名单，可对连接到白名单之外的无线网络行为进行阻断（提供截图证明，加盖原厂商章）。
4	边界管理	IP/MAC 绑定	具有入网设备自动学习功能，支持 IP/MAC/端口三者强制绑定，以及违规终端 VLAN 隔离机制，防止终端仿冒 IP 接入网络或移动设备位置。
		主机防火墙	终端在准入通过后访问域严格收管理员策略控制
			同网段终端无法互相访问，做到精确到端口的高安全性控制
5	设备私接管理	NAT 设备	▲具有 NAT 识别和检测机制能够及时发现网内私接的小路由器、无线 AP、随身 WIFI 等 NAT 设备，帮助清查通过网中网隐藏的真实网络终端（提供截图证明，加盖原厂商章）。
			对通过 NAT 入网的计算机可以实现准入控制、安全评估和修复等流程化管理提供截图证明，加盖原厂商章）。
		Hub 管理	能够发现内网私接的 Hub、傻瓜交换机等非网管设备，当多台计算机通过 Hub 接入网络时，能够及时产生告警通知管理员（提供截图证明，加盖原厂商章）。
			准入设备能够采用 VLAN 隔离、逻辑关闭端口等方式禁止 Hub 下联计算机接入网络。
			支持 Hub 下多个终端需分别认证才能入网和只需一台认证即可全部入网两种认证机制。
6	网络管理	设备识别	支持自动识别网络设备类型，包括：交换机、路由器、防火墙等，并按照类别自动进行归类。
			支持设备管理模板的定义功能，能够通过 SNMP、SSH、TELNET 等方式自动、批量添加网络设备。

		▲终端网络拓扑	准入设备支持交换机到终端计算机的网络拓扑管理功能，能够自动绘制出网络拓扑图（提供截图证明，加盖原厂商章）。
			能够在拓扑图上选取设备查看其基本状态信息、设备型号、所处位置、子节点、路由表、ARP 表等信息。
			支持在界面上提供对该网络设备进行 TELNET、SSH 等管理。
		交换机状态展现	支持可网管型交换机面板图形化展现各接口状态（up、down、trunk 等），以及各接口下联的终端详细信息（IP、地址、MAC 地址等）。
			能够支持自上而下逐级查找终端的具体位置、安全状态、认证用户、上下线时间等信息。
		AP 联动管理	能够与主流的 AP 设备深度联动，支持 AP 控制器面板的图形展现，包括 AP 连接状态、下联终端信息（IP 地址、MAC 地址等）等。
		DHCP 中继	能提供稳定的 DHCP 服务，并可以通过 DHCP 二次地址分配机制实现安全准入管理，支持交换机中继认证方式。
			能够根据用户、IP/MAC 绑定信息等条件，为指定终端设备分配特定的 IP 地址。
			支持 DHCP 服务器筛选，防止非法 DHCP 服务器分发错误地址
7	移动终端管理	终端识别	支持当前主流智能终端设备的安全准入控制，能够自动识别主流手机、智能终端等设备，并自动进行分类。
		移动终端入网	提供独立的智能终端入网引导界面的自主定制功能，至少包括界面标题、界面 LOGO、界面说明文字等。
			能够提供移动终端入网的设备注册功能。
8	认证管理	联动认证	能够全面结合用户已有的认证或业务系统，可以与 RADIUS、LDAP、STMP/POP 等采用标准协议的系统做深度联动认证。
		AD 域单点登录	能够与用户现有的 AD 域相结合，当用户登录到 AD 域后，无需二次认证即可入网，避免多次认证的繁琐流程。
			当用户未登录到 AD 域时，该终端将一直被隔离，该状态下只有通过 IE 页面进行认证才能够入网。
		证书认证	支持至少 2 个以上的根证书。终端用户认证时，自动进行认证证书的根证书匹配
		短信认证	支持短信认证模式，用户在登记入网手机号码后，能够在手机上接收到入网的短信验证码，并在 IE 页面上利用短信验证码认证入网。
		微信认证	通过关注微信公众号放行移动终端入网
		接入审核	能够针对不同的角色或设备类别有选择的开启入网审核功能，待审核的用户或设备必须经过管理员审批才能入网。
		认证控制	支持对认证时间段、IP 段控制限制某类（角色）账户只能在指定的时间段、IP 段认证。
		自助账号申请	支持用户在认证页面自行进行账号的申请。用户可自行提交用户名、密码、姓名、电话、部门、E-Mail 等信息。管理员审核通过后，用户即可使用该账号进行认证。有效解决用户账号和密码创建和分

			发的困难。
9	来宾管理	来宾角色	能够提供来宾角色选择，能够设定来宾设备的访问权限和入网时长
		来宾码认证	提供临时入网码，支持来宾设备与受访人员进行一对一绑定功能
		二维码认证	通过扫描二维码进行来宾入网管理
		来宾使用报表	生成来宾分配、来宾入网等动态审计报表
10	终端安全管理	安全检查库	准入设备提供系统安全配置、用户行为规范等类别检查项，至少提供 24 种以上安全检查项。
		系统补丁	▲准入设备具有完整的补丁管理子系统，无需第三方补丁服务器支持，自身可作为补丁服务器，自身即可以提供完整的流程化补丁管理，包括同步更新、补丁分类、补丁分发、补丁报表等功能（提供截图证明，加盖原厂商章）。
			能够在 IE 页面进行入网终端的补丁检查，补丁均划分为严重、重要、中等的类别，能够在 IE 页面显示出检查结果。
		防病毒软件	能够在 IE 页面检查出终端的杀毒软件情况，支持主流的 20 种以上的杀毒软件检查，包括微软 MSE、可牛、Avast 等，支持杀毒软件版本、病毒库和运行情况的检查，能够在 IE 页面显示出检查结果。
		Windows 组策略检测	windows 密码策略、屏保、共享目录、弱口令、防火墙、网卡配置等系统策略进行检查和修复
		计算机健康性检测	对终端的磁盘使用率、垃圾文件、IE 主页、网络监听端口等安全性配置进行检查和修复
		自定义安全检查	通过检测终端文件路径、指定文件版本、大小、MD5，注册表的项、注册表值，进程，服务名称、服务状态，进行检查。通过安装包运行、访问站点、开关服务、关闭进程、执行文件、删除文件、修改注册表进行修复。可以灵活的全访问的对终端进行安全检查和修复。
		终端安全加固	能够通过傻瓜式的漏洞修复模式为用户提供简单、形象的漏洞自我修复功能，完全不需要管理员的介入即可完成终端安全风险项修补。
		桌管系统联动	能够在 IE 页面检查出主流的桌面管理系统（包括 Landesk、北信源、威盾、盈高、圣博润等）客户端是否安装并正常运行，能够在 IE 页面显示出检查结果。
11	资源管理	软件检查	通过安全检查检测终端软件安装、使用状态
			自动强制为终端安装软件
			软件产品授权，支持进行 windows、office、WPS 的产品授权信息进行检查
		IP 地址管理	提供 IP 地址分配表，能够通过图示直观的查看各网段中未分配、开机、关机的数量和分布情况。
			能够直接、快捷的查看全网终端历史上线、下线、在线时长等详细的 IP 使用情况
		能耗管理	提供未关机终端自动统计功能，并能够按照部门、时间段等条件生成统计报表。

12	运维管理	移动终端管理	移动端管理平台可实现设备快速定位、设备审核、实时报警监控、小助手确认码生成、准入控制器管理、平台基本信息、关机与重启
		管理角色控制	准入设备须采用系统管理员、安全管理员、审计员三权分立机制，防止单个角色管理者权限滥用。
		网络诊断工具	支持通过 Web 管理界面提供 ping、抓包、traceroute、nslookup 等功能，并可以设置命令参数进行相关调试。
		消息群发	能够支持在指定的一台或者多台终端计算机上产生桌面消息通知，该消息会立即弹出在用户桌面上，对用户进行提醒。
		软件分发	准入设备应具有软件分发和部署功能，管理员可以预定义软件分发的路径、运行参数、是否执行等任务策略，以提升软件部署效率。
			能够自动判断并统计软件分发、部署的成功率，支持进程、注册表、安装路径等多种参数的组合判断。
13	报警报表管理	虚拟监控台	为了方便管理员从整体上把握网络安全态势，系统提供虚拟监控台功能。通过集中的仪表、数值显示快速进行安全态势的把握，主要包括：报警、安全风险等级、全网终端数、清理终端数、安检和规律、安检项状态分布。
		安全管理报表	准入设备后台能够按周、月、年统计安全状况走势图。
			准入设备后台提供每日入网报告、每周入网报告、每月入网报告。
		报警信息	可以提供紧急、重要、次要、提示等多个级别自定义报警模式。
			支持系统报警、网络报警、终端报警等类别，超过 20 种以上自定义报警类型。
			支持 Syslog 报警信息的定向输出。
		报警提醒	准入设备能够以邮件、手机短信、页面消息等多种报警方式提醒管理员各种安全异常状态。
14	▲第三方产品联动		支持与主流上网行为管理系统深度联动，构建内网准入、准出的全面安全管理体系。
			能够与主流动态口令认证系统相结合，提供动态密码联动认证机制。
			支持与国内外主流 U-Key 联动认证。
15	资质要求		公安部《计算机信息系统安全专用产品销售许可证-终端接入控制类》（提供证明文件，加盖原厂商章）
			国家保密局《涉密信息系统产品检测证书（网络访问控制产品）》（提供证明文件，加盖原厂商章）
			国家密码管理局《商用密码产品销售许可证》（提供证明文件，加盖原厂商章）
			中国信息安全认证中心《中国国家信息安全产品认证证书》（提供证明文件，加盖原厂商章）
16	▲保修		三年原厂硬件质保
17	▲其他		**提供原厂商授权函及售后服务承诺函（加盖原厂商章）**

（4）服务器接入交换机

序号	指标项	技术参数及技术要求
6	基本配置	10/100/1000Base-T 以太网端口≥24 个，其中 4 个复用的 1000Base-X 千兆 SFP 端口
7	性能	交换容量≥200Gbps，包转发率≥90Mpps
8	IP 路由	支持静态路由，支持 RIPv1/v2，支持 OSPFv1/v2
9	管理与维护	支持命令行接口（CLI）、Telnet、Console 口进行配置，支持 SNMPv1/v2/v3
10	保修	三年原厂硬件质保

四、其他相关要求

1、交货期：合同签订后 60 天内。

2、交付地点：用户指定地点。

3、采购资金的支付方式、时间、条件：

完成全部设备的供货，经甲方确认后，支付合同总金额的 30%，项目完成安装调试，经甲方验收合格后，支付合同总金额的 65%，剩余合同总金额的 5%转为质保金，质保期为 1 年，质保期结束后无息返还。

4、验收要求：按标书技术参数和国家行业标准进行验收。

5、售后服务要求：

(1)整体工程提供不少于三年的免费维护，设备按原厂商标准提供维护。

(2) 投标人或生产厂家须在国内设立服务机构，提供每周 7×24 小时技术支持和服务，针对使用过程中出现的故障问题，可以通过电话、网络方式先提供服务，2 小时内作出实质性响应，对重大问题提供现场技术支持，如果解决不了的情况下需要及时赶赴现场提供服务，8 小时内到达指定现场。

(3) 软硬件免费保修期，自验收合格之日起算。

(4) 保修期内非采购方人为因素而出现的质量问题，生产厂家负责保修、包换或者包退，并承担修理、调换或退货的实际费用。

(5) 投标人承诺提供的每一台设备均是全新的，厂家提供终身有偿维修、保养服务，保修范围外有偿维修，只收成本费。

(6) 投标人或生产厂家负责产品安装系统调试。

(7) 投标人或生产厂家负责长期提供技术资料和技术支持。

(8) 生产厂家保修期外需提供终身维护，设备故障维修只收取零配件费用。

(9) 投标人或生产厂家须对招标方使用人员及设备维修人员进行培训，使用人员能够熟练掌握设备的各项功能和操作，使维修人员能对设备进行日常维护和一般性故障的查找及故障的排除。

6、**由于项目实施过程会涉及招标方敏感信息，中标人必须提交保密承诺函。**

7、投标人必须根据所投产品的技术参数、资质资料编写投标文件。在中标结果公示期间，采购人有权对中标候选人所投产品的资质证书等进行核查，**如发现与其投标文件中的描述不一，代理机构将报政府采购主管部门严肃处理。**

用户需求书（B包）

一、项目名称

等级保护测评及信息安全服务

二、项目背景

通过委托专业的信息安全等级保护测评服务机构，对用户的信息系统安全保护等级进行需求分析，并协助用户完成等保备案相关事宜。依据《信息系统安全等级保护基本要求》，对信息系统的物理机房、网络结构、应用系统、主机、网络及安全设备等进行合规性检查，分析信息系統与安全保护等级要求之间的差距，出具《信息系统安全等级保护测评报告》，提出具有针对性的整改意见，并根据信息系统及安全防护措施的现状，提供渗透测试、安全管理体系建设服务、安全加固技术咨询服务、应急预案编制服务、应急演练服务及、网站云监测和云防护服务，确保信息系统的安全运行。

三、项目工期和地点

项目实施工期：采购人下达测评通知书后60个日历天内交付测评报告；

交付地点：用户指定地点。

四、等级保护测评服务需求

1、测评内容

（1）对用户的信息系统进行摸底、分析和梳理，提出详细的测评方案及完成系统备案工作。

（2）逐一对信息系统进行安全等级保护测评，测评的内容包括但不限于以下内容：

1）安全技术测评：包括物理安全、网络安全、主机系统安全、应用安全和数据备份及恢复等五个方面的安全测评；

2）安全管理测评：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五个方面的安全测评。

（3）完成测评工作后，提出整改方案；最后出具符合等保要求的网络安全保护等级测评报告，并协助用户完成网络安全保护等级备案工作。

2、 项目输出(包括但不限于以下内容)

（1）信息系统定级相关文件和报告；

（2）信息系统测评报告及整改建议；

（3）网络安全整改设计方案。

3、 测评对象描述

序号	被测系统名称	安全等级	被测系统描述
1	三亚市公安局门户网站	三级	三亚市公安局门户网站的功能包括信息展示、警务公开、便民服务、警民互动、赏金猎手、新闻发布、视频专栏、社区警务室等，业务办理模块包含交通管理办理、户政办理、出入境服务、治安管理业务、消防管理等。
2	三亚市公安局内网	三级	三亚市公安局内网是三亚公安业务的核心网络，该内网系统有两个专网出口，一个电信100M，一个移动100M，出口处做了边界路由冗余，防火墙串联边界路由做访问控制，再下连IPS 入侵防御，接入核心交换机，各楼层内网业务交换机通过汇聚交换机接入内网核心区，组成整个网络。
3	三亚市公安局视频监控系统	三级	三亚市公安局视频监控系统为适应社会经济、治安形势的发展，不断加强监控点、监控网络、监控中心、监控管理平台和监控机制建设，逐步建成一个覆盖各大型聚集场所、治安复杂区域和要害部位的社会面治安监控系统，全面提高公安机关掌握和控制社会面治安局势的能力。它可实现事故发生后的现场搜索、图像记录，以及疑犯跟踪等，更重要的是，它对犯罪份子起到了威慑的作用。与其他领域的监控系统相比，城市治安监控系统要求设备具有24小时连续工作的能力、稳定可靠性高，

4、测评服务步骤

信息系统等级保护测评过程需按照《信息系统安全等级保护测评过程指南》开展工作，等级测评过程分为四个基本测评活动：测评准备活动、方案编制活动、现场测评活动、分析及报告编制活动。测评双方之间的沟通与洽谈应贯穿整个等级测评过程。

（1）测评准备活动

测评准备工作包括编制项目启动、信息收集和分析、工具和表单准备。

详细要求见下表：

项目内容	工作内容	成果输出
项目启动	1.组建测评项目组	向用户提交 《项目计划书》《提供资料清单》
	2.编制《项目计划书》	
	3.确定测评委托单位应提供的资料	
信息收集分析	定级报告及整改方案分析	《系统基本情况分析报告》
	1.整理调查表单	

	2.发放调查表单给测评委托单位	
	3.协助测评委托单位填写调查表	
	4.收回调查结果	
	5.分析调查	
工具和表单准备	1.调试测评工具	确定测评工具（测评工具清单）《现场测评授权书》 《测评结果记录表》 《文档交接单》
	2.模拟被测系统搭建测评环境	
	3.模拟测评	
	4.准备打印表单	

（2）方案编制活动

方案编制活动包括测评对象确定、测评指标确定、测试工具接入点确定、测评内容确定、测评指导书开发及测评方案编制等六项主要任务。

详细要求见下表：

工作内容	工作详细任务	输出成果
一、测评对象确认	识别被测系统等级 识别被测系统的整体结构 识别被测系统的边界 识别被测系统的网络区域 识别被测系统的重要节点和业务应用 确定测评对象	《测评方案》的测评对象部分
二、测评指标确定	识别被测系统业务信息和系统服务安全保护等级	《测评方案》的测评指标部分
	选择对应等级的安全要求作为测评指标	
	就高原则调整多个定级对象共用的某些物理安全或管理安全测评指标	
三、工具测试点确定	确定工具测试的测评对象 选择测试路径 确定测试工具的接入点	《测评方案》的测试工具接入点部分
四、测试内容确定	识别每个测评对象的测评指标	《测评方案》的单项测评实施和系统测评实施部分
	识别每个测评对象对应的每个测试指标的测试方法	
五、测评指导书开发	从已有的测评指导书中选择与测评对象对应的手册	《测评方案》的测评实施手册部分
	针对没有现成测评指导书的测评对象，开发新的测评指导书	
六、测评方案编制	描述测评项目基本情况和工作依据	向用户提交 《测评方案》
	描述被测系统的整体结构、边界和网络区域	
	描述被测系统的重要节点和业务应用	
	描述测评指标	
	描述测评对象	
	描述测评内容和方法	

（3）现场测评活动

现场测评活动通过与测评委托单位进行沟通和协调，为现场测评的顺利开展打下良好基础，然后依据测评方案实施现场测评工作，将测评方案和测评工具等具体落实到现场测评活动中。现场测评工作应取得分析与报告编制活动所需的、足够的证据和资料。

现场测评活动包括现场测评准备、现场测评和结果记录、结果确认和资料归还三项主要任务。

详细要求见下表：

工作内容	工作详细任务	输出
1.现场测评准备	现场测评授权书签署	会议记录、确认的授权委托书、更新后的测评计划和测评方案
	召开现场测评启动会	
	双方确认测评方案	
	双方确认配合人员、环境等资源	
	确认信息系统已经备份	
	测评方案、结构记录表格等资料更新	
2.现场测评和结构记录	依据测评指导书实施测评	访谈结果：技术安全和管理安全测评的测评结果记录或录音 文档审查结果： 管理安全测评的测评结果记录 配置检查结果： 技术安全测评的网络、主机、应用测评结果记录表格 工具测试结果： 技术安全测评的网络、主机、应用测评结果记录，工具测试完成后的电子输出记录，备份的测试结果文件 实地察看结果： 技术安全测评的物理安全和管理安全测评结果记录 测评结果确认： 现场核查中发现的问题汇总、证据和证据源记录、被测单位的书面认可文件
	记录测评获取的证据、资料等信息	
	汇总测评记录，如果需要，实施补充测评	
3.结果确认和资料归还	召开现场测评结束会	
	测评委托单位确认测评过程中获取的证据和资料的正确性，并签字认可	
	测评人员归还借阅的各种资料	

（4）报告分析及编制活动

在现场测评工作结束后，应对现场测评获得的测评结果（或称测评证据）进行汇总分析，形成等级测评结论，并编制测评报告。

测评人员在初步判定单元测评结果后，还需进行整体测评，经过整体测评后，有的单元测评结果可能会有所变化，需进一步修订单元测评结果，而后进行风险分析和评价，形成等级测评结论。分析与报告编制活动包括单项测评结果判定、单元测评结果判定、整体测评、风险分析、等级测评结论形成及测评报告编制六项主要任务。

详细要求见下表：

工作内容	工作详细任务	工作依据（模版)
1.单项测评结果判定	分析测评项所对抗威胁的存在情况	等级测评报告的单项测评结果部分
	分析单个测评项是否有多方面的要求内容，依据“优势证据”法选择优势证据，并将优势证据与预期测评结果相比较	
	综合判定单个测评项的测评结果	
2.单元测评结果判定	汇总每个测评对象在每个测评单元的单项测评结果	等级测评报告的单项测评结果汇总分析部分
	判定每个测评对象的单元测评结果	

3.整体测评	分析不符合和部分符合的测评项与其他测评项（包括单元内、层面间、区域间）之间的关联关系及对结果的影响情况	等级测评报告的系统整体测评分析部分
	分析被测系统整体结构的安全性对结果的影响情况	
4.风险分析	整体测评后的单项测评结果再次汇总	等级测评报告的风险分析部分
	分析部分符合项或不符合项所产生的安全问题被威胁利用的可能性	
	分析威胁利用安全问题后造成的影响程度	
	为被测系统面临的风险进行赋值	
	评价风险分析结果	
5.等级测评结论形成	统计再次汇总后的单项测评结果为部分符合和不符合项的项数	等级测评报告的等级测评结论部分
	形成等级测评结论	
6.测评报告编制	概述测评项目情况	等级测评报告 提交用户
	描述被测系统情况	
	描述测评范围和方法	
	描述整体测评情况	
	汇总测评结果	
	描述风险情况	
	给出等级测评结论和整改建议	

五、渗透测试服务需求

借鉴黑客攻击的手法和技巧，在可控的范围内分别对公安网、视频监控网络、门户网站或整个内网进行模拟测试，全面挖掘漏洞，提供渗透测试报告。

渗透测试方法包括但不限于信息收集、端口扫描、口令猜测、远程溢出、本地溢出、脚步测试、权限获取等。

渗透测试是专业技术人员利用多种专业漏洞扫描工具对网络、操作系统、数据库、WEB 系统等进行交叉扫描验证，专业技术人员在对结果进行分析并人工对可能存在的漏洞点进行检查和模拟黑客攻击，帮助用户及时掌握信息系统安全状况，发现存在的主要问题和薄弱环节，并对发现的安全隐患提供改善建议，以及时帮助客户堵塞安全漏洞，协助指导客户落实和完善安全措施，以帮助客户建立信息安全保障机制，减少安全风险，提高应急处置能力，从而促进信息系统持续安全稳定运行。

六、安全管理体系建设服务需求

根据《BG-T22239-2008 信息系统安全等级保护基本要求》中的三级要求，结合单位的实际管理需求，调整原有信息安全管理模式和信息安全管理策略，对安全管理制度和规范流程进行梳理、调整和编制，构建满足信息安全等级保护的安全管理体系,制度至少包含以下内容：安全策略和管理制度、岗位设置、人员配备、授权审批、沟通合作、

审查和检查、人员录用、人员离岗、安全意识教育和培训、外部人员访问管理、定级和备案、方案设计、产品采购和使用、软件开发管理、工程实施、测试验收、系统交付、等级测评、供应商选择、环境管理、资产管理、介质管理、设备维护管理、漏洞和风险管理、网络和系统安全管理、恶意代码防范管理、配置管理、密码管理、变更管理、备份和恢复管理、安全事件处置、应急预案管理、外包运维管理。

服务结果输出

《安全管理制度汇编》,汇编中至少包含以下制度：

1.《信息安全组织机构》

2.《信息安全组织建设规定》

3.《用户密码管理制度》

4.《信息化安全建设目标及组织机构管理办法》

5. 《人员安全管理》

6.《岗位职责管理规定》

7.《办公环境管理制度》

8.《管理评审制度》

9.《保密协议》

10.《产品选型指导办法》

11.《系统安全管理制度》

12.《信息系统变更控制管理制度》

13.《口令使用规定》

14.《介质管理制度》

15.《文件控制制度》

16.《项目验收检查流程》

17.《信息类设备标识管理办法》

18.《信息安全奖惩管理规定》

19.《信息资产管理制度》

20.《信息系统管理维护制度》

21.《信息系统建设管理制度》

22.《机房管理制度》

23.《防病毒管理制度》

24.《日志审计管理办法》

25.《设备管理制度》

26.《网络安全管理制度》

27.《网络设备安全配置管理规定》

28.《信息系统开发与维护管理制度》

29.《信息系统外包管理制度》

30.《资产备份恢复管理制度》

31.《基础设施故障处理流程》

32.《安全事件管理制度》

33.《突发事件应急制度》

34.《网络故障应急处理流程》

编制后的制度必须符合最新的等级保护规范中的三级要求。

七、安全加固技术咨询服务

依据《信息系统安全等级保护基本要求》并结合三亚市公安局信息安全现状、测评过程中发现的问题，从物理安全、网络安全、主机安全、应用安全、数据安全及备份恢复等方面提供安全加固技术咨询服务，服务内容包括漏洞修复、策略优化、结构调整、配置加固、规划设计等，旨在从软技术上加强三亚市公安局网络与信息系统安全防护水平，能够抵御网络入侵和攻击，防止信息网络瘫痪、应用系统被破坏、业务数据丢失、数据泄露、终端病毒感染、有害信息传播，确保信息系统安全稳定运行，确保业务数据安全。

八、应急预案编制及应急演练服务

应急预案及应急演练服务将根据《中华人民共和国突发事件应对法》、《突发事件应急预案管理办法》、国家信息安全等级保护标准《信息安全等级保护基本要求》（GB/T22239--2008）、《中华人民共和国网络安全法》、《海南省信息化条例》和《关于印发海南省党政机关、事业单位和国有企业互联网网站安全专项整治行动方案的通知》等文件对“信息安全事件应急响应、应急预案和应急演练”的相关规定，结合用户信息系统的实际情况，指导用户建立健全信息与网络安全事件应急响应工作机制，并对信息系统相关人员进行应急预案、应急技巧及对典型的信息安全事件进行预防等方面的培训。

信息安全事件应急预案包括以下安全事件：

有害程序事件：计算机病毒事件、蠕虫事件、特洛伊木马事件、僵尸网络事件、混合攻击程序事件、网页内嵌恶意代码事件和其它有害程序事件；

网络攻击事件：拒绝服务攻击事件、后门攻击事件、漏洞攻击事件、网络扫描窃听事件、网络钓鱼事件、干扰事件和其他网络攻击事件；

信息破坏事件：信息篡改事件、信息假冒事件、信息泄漏事件、信息窃取事件、信息丢失事件和其它信息破坏事件；

信息内容安全事件：违反宪法和法律、行政法规的信息安全事件；针对社会事项进行讨论、评论形成网上敏感的舆论热点,出现一定规模炒作的信息安全事件；组织串连、煽动集会游行的信息安全事件；其他信息内容安全事件；

设备设施故障：软硬件自身故障、外围保障设施故障、人为破坏事故、和其它设备设施故障。

信息安全事件应急预案演练主要对运行环境安全、网络结构安全、设备运行安全、系统可用性、外界风险因素等各方面进行全面演练，主要覆盖重要信息系统、数据中心、灾备中心等重要基础设施，重要服务商应急保障能力，外部应急协调机制等。

做到全面演练和专项演练相结合。应急演练应贴合信息系统的实际情况，主要的演练方式为模拟演练及桌面演练。

演练场景以可能出现的通讯故障、系统故障、系统安全等为重点，结合用户实际情况和关键风险点，设计以下应急场景进行演练：

通讯故障：演练在用户量激增、网络设备故障、通信线路被破坏、网络受到攻击等原因导致通讯中断和拥塞时的应急预案以及与公安、电信部门的应急协调与保障机制。

系统安全：演练因病毒爆发、网络入侵攻击、篡改网站等情形下的系统应急预案以及与公安、电信部门的应急协调机制。

系统故障：主要演练主要信息系统出现应用故障、数据库故障、存储设备故障、主机硬件故障等的应急预案以及外联单位、系统重要服务商的应急协调与保障能力；检验外联单位相关系统的应急保障能力。

九、网站云监测和云防护服务

针对三亚市公安局门户网站，提供 1 年的 7X24 小时云安全防护及监测服务。服务内容包括： Web 攻击防护、抗 DDOS 攻击（10Gbps）防护、抗 CC 攻击（10000Q/S）防护、可用性监测、漏洞监测、网页篡改监测、网页挂马监测、内容变更监测、黑词监测、黑链监测、敏感词监测、可用性云监测、提供报表和通报功能。

十、项目服务要求

1、项目实施要求

项目实施过程中，投标人应遵循国家标准、行业标准。

在项目实施中投标放须做到：

（1）本项目的项目经理必须具有 1 年以上的等保测评服务项目管理经验；其中，本项目成员中至少有 2 人具备信息安全等级保护中级测评师资格；

（2）提供完整的系统实施方案和项目实施管理办法；

（3）提供详细的项目实施方案和计划进度说明书；

（4）项目实施完成后提供可靠的后期技术服务工作；

（5）严格按照双方确定的计划进度保质保量完成工作；

（6）规范项目实施过程中的文档管理。

2、项目验收要求

中标方必须提供给业主详细的项目验收方案。

（1） 验收组织

成立由招标方、中标方以及其他有关人员组成的验收小组，负责对项目进行全面的验收。

（2）验收标准

1）标准化：项目验收最关键的指标，应确保测评过程符合国家标准规范；

2）系统稳定性：在测评过程中应确保软硬件环境的稳定性、运行正常；

3）系统文档：验收文档是否齐全、规范、准确、详细；

4）系统可操作性：交付成果清晰、通俗易懂。

（3）售后服务要求

对于评估中发现的应用系统、主机和网络设备漏洞，中标方应提供项目验收后一年内的跟踪服务，对本次评估范围内的问题提供远程或现场技术咨询，对于漏洞的修补、问题的排除给出建议和指导。