信息化网络基础建设项目用户需求

一、建设总体目标

海南省森林公安的信息化基础设施建设包括传输链路带宽的提升以及各级网络设备的升级改造建设，升级改造省森林公安局、林区（保护区）森林公安局、市县森林公安局、派出所网络设备。将省森林公安局至省公安厅的网络出口传输链路带宽需提升至千兆，完善与省公安厅的网络互通能力；将林区（保护区）森林公安局、市县森林公安局至当地公安局的传输链路带宽需提升至百兆，完善与当地公安局的网络互通能力；63 个森林公安派出所至所在分局的传输链路带宽需提升至百兆，完善提高基层网络传输效率与能力。对于各级网络设备的建设，根据海南森林公安的网络现状以及需求分析，需要构建一张从省局、分局到派出所的安全可靠的广域网网络，并且具备高拓展性、高可靠性、高安全性，实现省局业务与各个分局、派出所之间实现互联互通。同时，将完善森林公安网络的安全管理，加固森森公安网络安全，保障信息安全。

二、本项目建设目标

通过本项目的建设，完成从省局到各公安分局及派出的网络设备、安全设备的升级改造建设，完善省森林公安局与省公安厅的网络互联互通能力；完善 24 个林区（保护区）森林公安局、市县森林公安局与当地公安局的网络互联互通能力；提升 63 个森林公安派出所至分局网络传输效率与能力。最终提高海南省森林公安的信息化支撑和保障能力，实现森林公安内部各种数据的安全、流畅传送，为下一步森林公安的移动执法、移动安全接入管理奠定坚实的网络基础。

建设网络信息安全设备，保障森林公安网络安全，提高信息系统的信息安全防护能力，降低系统被攻击的风险。

三、建设需求

3.1、网络传输需求分析

- 可靠的业务服务质量保证

公安信息网集平台网页浏览、数据库查询、协同办公、视频会议等应用类型。当网络流量处于高峰期时，会对关键业务数据流的产生影响，如何保障重要业务高质量服务，提高森林公安的网络运行和体验，是森林公安信息化网络组网建设需要关注的重要环节。

- 具备端到端的服务保障

具备 QoS 能力，提供业务的 QoS 保障满足语音、视频等业务对带宽、时延、抖动、丢包率等参数的要求。

3.2、网络管理需求分析

- 分支数量多

数量繁多的分支极易造成大量耗费人力物力的重复性劳动，极大的降低了上线效率；

- 地理位置分散

分布于全岛各市县、各林区等的分支使得出差式上线成为唯一可行性方法，交付成本超过设备本身的购买成本；

- 没有部署能力

分支（市县直属分局、派出所）无专业运维人员，需通过纯人工出差的方式才能进行复杂的预上线配置，无法适应时效性极强的业务发展；

3.3、网络安全管理需求分析

网络系统应具有良好的安全性，由于公安网络的特殊性，安全管理十分重要。网络具有防止及便于捕杀病毒功能。应支持 VLAN 的划分，并能在 VLAN 之间进行第三层交换时进行有效的安全控制，以保证系统的安全性。

大部分用户重视省局端数据中心的安全建设而忽略了分支机构的安全防护，以下是广域网常见的五大安全风险：

- 边界安全：存在被攻击的风险，特别是未知威胁等新型攻击很容易绕过传统边界防御；
- 传输安全：没有加密的数据传输存在被监听、拦截、窃取的风险；
- 行为安全：内部员工安全管理，行为审计，做到合法合规；
- 移动安全：移动办公存在泄密风险；
- 终端安全：分支终端经常被称为黑客的“养马场”；

四、建设内容

本项目主要是对海南省森林公安的信息化基础设施（网络及安全系统）进行升级改造建设，提高海南省森林公安的信息化支撑和保障能力。总体建设内容包括，完善省森林公安局至省公安厅的网络出口能力，完善与省公安厅的网络互通能力；同时，

对省森林公安局、林区（保护区）森林公安局、市县森林公安局的网络安全进行防护和加固，并对整张广域网络进行有效管理，完善分局与省局之间的网络互通；此外，完善派出所与分局、省局之间的安全可靠的互联互通，实现森林公安内部各种数据的安全、流畅传送，为下一步森林公安的移动执法、移动安全接入管理奠定坚实的网络基础。

本期项目建设内容如下：

1. 省森林公安局网络设备升级改造及信息安全系统建设；

2. 24 个市县（林区）森林公安局网络设备升级改造及安全系统建设；

3. 63 个森林公安派出所网络设备升级改造建设。

五、项目参数技术要求

5.1、省森林公安局

序号	货物名称	数量	技术参数及性能配置要求
1.	网络安全系统		
1	省森林公安局出口下一代防火墙	1 台	1. 网络层吞吐量 8G，并发连接≥230 万，每秒新建连接数 15 万， 标准 2U 机箱，冗余电源，标准配置 6 个 10/100/1000M 自适应电口，另有 2 个接口板卡扩展插槽，1 个 Console 口，支持液晶屏；配置 128GB SSD 固态硬盘存储，三年病毒防护特征库升级服务，三年入侵防御特征库升级服务，含三年硬件维保服务。 2. 所投产品支持 MPLS 流量透传，并支持检测、防护 MPLS 流量中的安全威胁 3. 所投产品支持 MTU≥9000byte 的巨型帧通过设备传输时不分段 4. 所投产品必须支持基于 IP、应用、服务的策略路由进行智能选路，支持源地址目的地址哈希、源地址哈希、时延负载、最优链路带宽负载、最优链路带宽备份、跳数等不少于 12 种路由负载均衡方式。 5. 所投产品必须支持不少于 8 条链路的 ISP 路由负载均衡，支持自定义链路负载权重，支持基于优先级的 ISP 路由链路备份；支持不少于 4 种的链路状态探测机制，实现失效链路快速切换 6. 所投产品支持 SNAT、DNAT。支持在源地址转换过程中，对 SNAT（源地址转换）使用的地址或地址池利用率进行监控，并在地址池利用率超过阈值时，通过 SNMPTrap、邮件、声音、短信等方式告警。 7. 所投产品必须支持基于源安全域、目的安全域、源用户、源地址、源地区、目的地址、目的地区、服务、应用、隧道、时间、VLAN 等多种方式进行访问控制，并支持地理区域对象的导入以及重复策略的检查。 8. 支持基于不同安全区域防御 DNSFlood、HTTPFlood 攻击，并支持警告、阻断、首包丢弃、TC 反弹技术、NS 重定向、自动重定向、手工确认等多种防护措施。 9. 所投产品应具备本地、云端双擎查杀能力，必须能够对 HTTP/FTP/POP3/SMTP/IMAP/SMB 六种协议进行病毒查杀，以及对至少 6

序号	货物名称	数量	技术参数及性能配置要求
			级压缩文件进行解压查杀 10. 所投产品必须支持针对 FTP、HTTP、IMAP、OTHER_APP、POP3、SMB、SMTP 等应用协议的漏洞攻击防护功能，至少可防御缓冲区溢出、跨站脚本、拒绝服务、恶意扫描、SQL 注入、WEB 攻击等类型的攻击 11. 所投产品应内置高质量漏洞攻击特征，应能够防御“永恒之蓝”、“震网三代”、“暗云 3”、“Struts”、“Struts2”、“Xshell 后门代码”等高危流行漏洞；漏洞特征应具备丰富的描述信息，至少包括对应的攻击的名称、CVEID、CNNVDID、严重性、影响的平台、类型、描述等详细信息 12. 所投产品支持配置虚系统，支持在虚系统内独立配置病毒防护、漏洞利用防护、间谍软件防护、URL 过滤、文件过滤、内容过滤、邮件过滤、行为管控等安全功能。并可支持对本虚系统内产生的日志进行独立审计 13. 所投产品必须提供关联的威胁事件日志，系统可自动将产生威胁事件的连接经过防病毒、防漏洞、防间谍软件、URL 过滤、文件过滤等安全模块检查的日志集中显示，并支持对全部类型的日志模糊或精确检索。 14. 支持与云端联动，至少实现病毒云查杀、URL 云识别、应用云识别、云沙箱、威胁情报云检测等功能 15. 具备公安部网络安全保卫局颁发的《计算机信息系统安全专用产品销售许可证》（增强级）（提供证明材料并加盖厂商公章） 16. 具备国家信息安全测评中心颁发的《信息技术产品安全测评证书》（EAL4+）（提供证明材料并加盖厂商公章） 17. 《中国国家信息安全产品认证证书》（提供证明材料并加盖厂商公章）
2	日志审计系统	1 台	1. 性能：事件采集 10000EPS，事件处理最高 3000EPS。硬件规格：标准 1U 机箱，6 个千兆电口，2 个扩展插槽，1 个 Console 接口，冗余电源，4T 硬盘。包含 50 授权节点，包含三年标准维保。 2. 支持单一部署，也支持级联部署，管理中心内嵌数据库，用户无需另外安装数据库管理系统。 3. 支持通过 syslog、snmptrap、netflow、jdbc、odbc、agent 代理、wmi 等多种方式完成各种日志的收集功能 4. 系统应提供从总体上把握日志告警和日志统计分析的实时综合性监控界面，用户可以自定义监控主页。 5. 系统支持自定义资产属性；支持对资产日志进行过滤，设置允许接收和拒绝接收日志，并可以对资产设置一定时间范围内未收到事件后进行主动告警。 6. 支持采集一化后的日志和保留原始日志，方便用户对关键日志快速定位，和事后取证；日志收集后进行字段和安全等级的归一化处理，系统归一化字段不少于 50 个字段,并至少有 8 个可自定义字段。 7. 支持对事件名称、源地址、源端口、目的地址、目的端口相同的进行归并，条件可以多种组合；支持对指定设备发送的日志进行归并，其他设备发送的将不进行归并；支持对事件个数深度和事件时间深度进行归并。 8. 支持实时的日志滚动显示，可通过趋势图等直观显示目前日志量和日志详细信息。支持对实时展示的字段进行选择，调整字段顺序，修改显示字段别名。 9. 支持鼠标放在日志对应字段上界面可悬浮提示资产信息和常用端口信

序号	货物名称	数量	技术参数及性能配置要求
			息。 10. 支持自定义实时分析场景，提供可视化规则编辑视图，根据实际业务编写分析规则。 11. 能够在世界地图上实时定位事件源/目的 IP 地址的地理位置。 12. 可对不同类型设备的日志之间进行关联分析，支持递归关联，统计关联，时序关联，这几种关联方式能同时应用于一个关联分析规则。 13. 系统预置知识库，IP 地理库，漏洞库。 14. 日志转发支持设置过滤条件选择对转发的日志进行过滤。 15. 支持禁止与允许用户访问日志审计系统的 IP 地址限制，支持 raidus 认证。 16. 系统支持 WEB 界面锁定，锁定后界面不允许操作，需要操作需要输入密码。 17. 产品需要提供公安部《计算机信息系统专用产品销售许可证》。（提供证明材料并加盖厂商公章） 18. 产品需要提供中国信息安全认证中心《中国国家安全产品认证证书》3C。（提供证明材料并加盖厂商公章） 19. 产品需要提供国家信息安全测评中心《信息技术产品安全测试证书》EAL3+。（提供证明材料并加盖厂商公章）
3	运维审计系统	1 台	1. 6 个千兆电口,支持 2 个接口扩展槽位，内置 4TB 硬盘，支持液晶屏，最大支持 150 路图形会话或 400 路字符会话并发。含三年标准售后服务。授权 50 个被管资源数。 2. 物理旁路，逻辑串联模式，不影响原有网络架构。 3. HA 双机热备、支持跨地域、跨数据中心，多层次部署。 4. 支持 SSH、RDP、VNC、Telnet、FTP、SCP、SFTP、DB2、MySQL、Oracle、SQLServer、Rlogin 等协议。 5. 支持 IPv6 网络环境下的运维、操作审计。 6. 支持按 IP 范围、端口进行资源设备自动发现，实现快速批量添加资源设备。 7. 不限操作客户端系统类型，无需安装任何客户端插件，使用 H5 即可直接运维 windows、Linux、网络设备等资源。 8. 运维过程中支持会话协同，可邀请其他用户参与、协助操作。 9. 支持本地、RADIUS 和 AD 域等认证方式 10. 支持动态令牌、USBKEY、手机令牌、手机短信等多因子认证。 11. 支持按用户、账户组设置多对多的资源访问授权，用户组和账户组内的新增成员自动继承授权关系。 12. 预制 Linux 主机和网络设备的基本命令，支持正则表达式和通配符方式设置匹配规则，自定义命令黑白名单。 13. 支持用户水印功能，避免数据泄露无法追责 14. 支持对运维操作中的详细操作命令、步骤、以及双人授权、协同用户、剪切板拷贝行为进行记录，并可以通过关键字搜索定位回放，审计日志内容支持导出。 15. 支持自动修改资源服务器账户密码，系统类型包括 Windows/Linux/Unix/Cisco/Huawei/H3C，等网络设备，数据库类型包括

序号	货物名称	数量	技术参数及性能配置要求
			MySQL、Oracle、SQLServer 等。 16. 支持随机生成不同、相同密码或者手动指定密码，改密日志内容包括改密账户总数，成功、失败和未修改数量。 17. 支持 web 和 SSH 登录无操作超时设置 18. 支绑定堡垒机用户公钥，实现客户端访问堡垒机免密码登录。 19. 具有《计算机信息系统安全专用产品销售许可证》（提供证明材料并加盖厂商公章） 20. 产品需要提供中国信息安全认证中心《信息安全产品认证证书》。（提供证明材料并加盖厂商公章）
4	漏洞扫描系统	1 台	1. Web 扫描域名无限制，Web 扫描任务并发数为 5 个域名。系统扫描 IP 地址无限制，支持扫描 A 类、B 类、C 类地址，系统扫描支持 50 个 IP 地址并行扫描。机架式，1T 硬盘，配置 6 个 10/100/1000M 自适应电口，2 个扩展插槽,2 个 USB 口，1 个 Console 口。包含三年漏洞特征库升级，三年硬件维修服务. 2. 产品具备 B/S 架构设计，并采用 SSL 加密通信方式，用户可以通过浏览器远程方便的对产品进行管理。 3. 产品具备多路并行扫描机制，可以同时对多个隔离网络进行漏洞扫描 4. 产品具备分布式部署需支持自定义管理中心端口号、策略端口号、远端扫描引擎名称等信息 5. 产品具备分布式部署提供远端扫描引擎列表，列表需对设备状态、策略同步、规则同步、引擎类型等状态提供最直观的展示效果 6. 产品具备以树形结构方式管理，针对树形结构的资产呈现资质风险 7. 产品具备支持未知资产探测发现功能，提供基于对 IP、端口的探测功能 8. 产品应具备操作系统、数据库、网络设备等主流系统的漏洞库列表，并提供至少 20 种以上的漏洞库分类 9. 产品漏洞库列表数量必须大于 20000 条，提供详细的漏洞描述和对应的解决方案描述；漏洞知识库与 CVE、CNCVE、CNNVD、CNVD、Bugtraq 等主流标准兼容 10. 产品具备对 DNS 服务、后门检测、常见 P2P 软件等安全漏洞检测 11. 产品具备对网页暗链、敏感词汇、网站木马的检测 12. 产品需支持对 Web 网站漏洞扫描的同时，查看网站漏洞情况和 Web 目录结构，数据进行实时同步呈现 13. 产品具备专用的口令破解字典，包括密码字典、用户名字典、组合字典等多种口令破解字典 14. 产品具备 SMB、TELNET、FTP、SSH、POP3、MSSQL、MYSQL、ORACLE、DB2、SNMP 等协议进行口令猜测 15. 产品具备专业配置核查的漏洞库，具备主流的操作系统、数据库、网络设备、安全设备的相关安全配置核查漏洞库 16. 产品具备公安部的信息系统等级保护的配置核查 17. 产品具备报表导出功能，提供 HTML、word、PDF、excel、XML 等 5 种报表格式，导出数据分为详细报表和统计报表 18. 产品具备自定义报表功能，提供对标题、信息、LOGO 等数据的自定义 19. 具有《计算机信息系统安全专用产品销售许可证》（提供证明材料并加

序号	货物名称	数量	技术参数及性能配置要求
			盖厂商公章） 20. 具有《中国国家信息安全产品认证证书（3C）》（提供证明材料并加盖厂商公章）
5	数据库审计	1 台	1. 事件处理 12000 条/秒，内置 4TB 磁盘存储空间。标准 1U 机箱，单电源；6 个千兆自适应电口，1 个 Console 口，支持两个扩展槽位，支持液晶屏。包含三年软件升级和硬件维修服务。 2. 系统可同时支持 IPv4 和 IPv6 的网络环境下数据库的审计。 3. 支持的数据库：Oracle、SQL-Server、DB2、Informix、Sybase、MySQL、PostgreSQL、达梦、人大金仓、南大通用 Gbase、Caché、REDIS。 4. 支持对 SQL 注入、跨脚本攻击、grant 语句进行提权行为的审计 5. 对审计记录返回内容中的敏感数据能进行隐秘处理，防止二次泄露。 6. 支持 B/S 架构 Http 应用三层审计，可提取包括应用系统的人员工号（账号）的身份信息，精确定位到人，并可获取 XML 返回结果。支持 C/S 架构 COM、COM+、DCOM 组件的三层审计，可提取应用层工号（账号）的身份信息，精确定位到人；支持框架：tomcat、apache、weblogic、jboss 7. 审计策略支持 18 种以上分项响应条件；可支持数据库操作命令（包括 select、create 等 14 个命令）；语句长度、语句执行回应、语句执行时间、返回内容、返回行数、数据库名、应用账户、服务器端口、客户端操作系统主机名、客户端操作系统用户名、客户端 MAC、客户端 IP、客户端端口、客户端进程名、会话 ID、关键字、时间（含开始结束日期）等 8. 内置疑似 SQL 注入、跨站脚本攻击、数据库导库、字段猜测、代码更改、等近 500 种风险审计规则库。 9. 支持全数据库检索，检索效率高达亿条数据秒级响应。 10. 可根据事件的时间范围、客户端 IP、关键字、进程名、应用账号、规则名、客户端端口号、返回内容等多种条件进行事件回放，回溯事件过程。 11. 支持对指定时间段风险数据按不同维度进行统计排行，统计维度包括：风险最多的类型、触发风险最多的保护对象、触发风险最多的 IP、触发风险最多数据库账户、触发风险最多应用账户、触发风险最多工具； 12. 支持对统计数据进行下钻，获取更详细的风险数据； 13. 系统可根据全方位对数据库的访问行为，评估被保护数据库的整体安全指数； 14. 系统支持在设备访问界面上展示具体的安全能力信息，协助管理员了解数据整体的安全状况。 15. 可根据保护对象、年份、月份进行统计以下报表：账户数最多的数据库 Top5 排名、连接数据库服务的访问者 IPTop5 排名、查询语句执行时间分布 Top5、繁忙的数据库服务器 Top5、执行时间最长的语句，同时支持 excel、word、pdf 格式报表的导出。 16. 提供用户界面告警、Syslog 告警、SNMP 告警、邮件告警、短信系统、短信猫告警等六种方式

序号	货物名称	数量	技术参数及性能配置要求
			17. 用户管理支持三权分立，系统提供了审计管理员、系统管理员、安全管理员分权的用户体系。 18. 具有《计算机信息系统安全专用产品销售许可证》（提供证明材料并加盖厂商公章） 19. 具有《中国国家信息安全产品认证证书（3C）》（提供证明材料并加盖厂商公章）
6	上网行为管理	1 台	1. 1U 硬件，标配 6 个千兆电接口（其中含 1 个管理接口和 1 个 HA 接口），提供 1 个扩展插槽，单交流电源。 建议 1000 人网络环境使用；最大并发连接数为 70 万，最大新建连接数为 24000 个/秒；含专用操作系统与上网行为管理标准软件。 含三年软件版本及协议库升级服务、三年硬件质保服务。 2. 设备必须提供物理硬件 bypass 按钮，便于设备巡检、设备故障时管理员无需重启、关机、断电即可恢复网络通畅。 3. 支持远程登录在界面实现 Bypass，并可进行切换。 4. 支持设备模式选择，可以设置为 Portal 模式实现 Portal 服务器功能。 5. 产品支持多台设备主主模式部署。 6. 能够支持 IPv6 环境下的网址访问审计、生成分析报表等功能；能够在 IPv6 环境下，正确审计显示用户的 IPv6 地址。 7. 支持基于云端大数据安全平台，对恶意 URL 访问进行封堵和记录日志。 8. 可以对下载工具、视频播放、网络游戏、金融理财、即时消息、移动应用有独立的分类进行识别控制。 9. 为覆盖工作无关应用，移动应用不少于 1000 种，即时消息应不低于 150 种，虚拟货币交易平台不低于 40 种。 10. 不同网页被阻塞后会跳转不同的阻塞页面；支持用户完全自定义。 11. 当用户的网页访问被网页浏览策略封堵时，用户如果发现分类错误能够在页面中向管理员进行反馈；管理员可查看用户反馈的分类错误，并可以选择向服务器反馈。 12. 一条策略可实现 Webmail 以及 SSL 加密的 Webmail 基于发件人、收件人、主题、内容、附件名维度的记录、阻塞、告警；能够基于发件人、收件人、主题、内容、附件名维度进行过滤、记录、告警；能够支持 SSL 加密的 SMTP 邮件审计。 13. 支持对 QQ、微信和百度网盘的 PC 客户端外发文件进行关键字过滤和封堵。 14. 支持多级虚拟通道，可以将物理带宽分成至少 7 级虚拟通道，合理分配物理带宽资源。 15. 可基于源 IP、用户、位置、终端台数、PC 台数、移动台数、阻塞时间和动作，配置多条共享接入策略。 16. 管理员登录支持登录失败次数配置和阻断时长配置。 17. 支持策略管理、日志审计、权限分配相互独立的三权制衡管理机制，避免超级管理员权限过大的弊端。系统管理员和审计员的账号创建，权限变更需要审核员审批才能生效。管理员和审计员的操作会形成日志受审核员监督。 18. 公安部网络安全保卫局颁发的《计算机信息系统安全专用产品销售许可

序号	货物名称	数量	技术参数及性能配置要求
			证》。（提供证明材料并加盖厂商公章） 19. 产品需要提供国家信息安全产品认证证书（提供证明材料并加盖厂商公章）
7	统一管理平台	1 台	1. 安全管理系统软件，提供系统的基础框架（平台核心服务、告警管理、报表管理、权限管理、系统配置），包括网络管理模块（网络拓扑发现模块、设备面板管理模块、机架物理视图管理模块）、网络设备监控模块、安全设备监控模块、服务器监控模块。平台内置数据库，包括 125 个监控节点许可，包含 3 年维保服务。含安装配置及调试服务。 2. 该系统为一套统一的、完整的软件产品，采用 B/S 架构。符合公安部“安全管理平台类”产品的检测规范(提供相关证明)。其中，管理中心内嵌数据库，用户无需另外安装数据库管理系统；管理客户端基于浏览器，无需安装其他客户端软件。 3. 能够集中监控网络中的主机设备、网络设备、安全设备、应用系统。具体包括：交换机、路由器、防火墙、Windows 服务器、AIX 服务器、Linux 服务器、HP-UX 服务器、Solaris 服务器、SQL Server、Oracle、DB2、Sybase、MySQL 数据库系统、webshpere/ weblogic 中间件、Mail/Web/FTP/DNS/DHCP/WINS 和 LDAP 服务等。 4. 可对网络中的 IP 资产进行管理，支持以安全域的方式对资产进行分组，资产的属性包括安全 CIA 指标，支持自定义资产属性，可根据需要对资产属性进行任意扩展。 5. 支持网络拓扑发现，自动生成网络拓扑图，支持分层显示和全局显示两种展现方式。在全局显示模式下，能够在一个拓扑图上显示三层、二层网络设备和终端设备。拓扑图上能够显示节点之间的链路连接，并标示流量值。如果节点出现故障，拓扑图节点能够显示为红色。支持对拓扑图的鸟瞰、缩放、导出、导入、更换底图、编辑。内置 ping、tracerouter、telnet 等常用工具，可直接调用。通过拓扑地图，用户可以调用设备的 http 接口、telnet 接口、ssh/ssh2 接口实现对设备的直接访问和控制。 6. 用户可以看到设备的面板图，并可以针对面板上的接口进行实时监控和设置，进行形象化管理。 7. 能对包括服务器和 HP、IBM 小型机在内的各种主机操作系统进行监控。不仅能够检测主机性能，还能够检测主机安装的软件信息、在线用户信息、主机进程信息、主机网络连接信息、主机服务运行信息等 8. 能够对主机运行的进程信息进行实时监控。通过将进程信息与进程黑名单比对，发现主机上正在运行的违规进程。通过将进程信息与进程白名单比对，进行主机进程防御基线管理 9. 网络设备属性，网络设备状态监控，网络性能监控，cpu 利用率监控，内存利用率监控，接口监控，设备面板管理，可以对重点设备的重点端口进行流量监控，并且可以配置告警阈值。对于端口流量，管理员可以根据自定义的时间段生成流量报表 10. 支持数据库运行状态信息和库性能信息进行监控，支持 Mysql、SQL serve、DB2、Oracle、Informix、Sybase。 11. 支持对中间件服务状态和性能信息，支持 WebSphere、WebLogic、Tomcat、Jboss、Apusic、WebSphereMQ、Tuxedo。

序号	货物名称	数量	技术参数及性能配置要求
			12. 在实时监视中，对于关联事件，用户可以进行追溯，查看导致该关联事件的所有原始事件 13. 系统能够将数千条事件记录及其这些事件之间的关联关系变成一幅事件图，形象地展现出当前网络安全状态，一目了然 14. 在实时监视中，管理员通过事件调查工具可以对某条感兴趣的日志中的源 IP 地址、目的 IP 地址、或者目的端口进行相关性日志检索。 15. 用户在实时监视的过程中如果发现某条事件的相关属性需要持续予以关注，可以将该事件分配到黑白名单中。 16. 提供可视化的规则编辑器，利用编辑器，可灵活方便地生成任意关联分析规则。 17. 自动采集和存储 IT 计算环境中的各类告警信息，并将所有的告警记录按发生时间、告警状态、事件类型、事件等级、源设备 IP、源设备类型等信息列表显示，对告警信息进行分析和统计。产生的告警信息能够通过邮件、短信、控制台弹出窗口、snmp trap、执行预定义参数脚本程序的方式进行自动化响应。 18. 通过角色定义支持多用户访问 19. 公安部《计算机信息系统安全专用产品销售许可证》（提供证明材料并加盖厂商公章） 20. 国家版权局《计算机软件著作权登记证书》（提供证明材料并加盖厂商公章）
2. 网络设备系统			
1	网络管理软件	1 套	1. 系统支持 B/S 架构，支持组件化安装模式，可根据业务需要进行按需安装。浏览器需支持 IE、FireFox、Chrome 等业界主流浏览器。 2. 系统需要支持 Windows Server 2008 R2 标准版、Windows Server 2012 R1 标准版、Novell SUSE Linux Enterprise Server-企业版-11.0 SP3 等业界广泛使用的操作系统，并提供持续的补丁更新。 3. 系统需采用业界主流的数据库软件，如 MySQL、SQL Server 2008、Oracle 等。为提高整体方案安全性，系统需支持数据库独立部署以及集中式部署两种方式。 4. 系统需支持大规模管理能力，单套管理能力不低于 18000 台网络资源。 5. 系统支持分级部署，下级网管数量最大可以支持 500 个，整网最多可以管理 280,000 台设备。 6. 实配：100 个网络设备管理 license 7. 系统需支持单机部署、双机部署等多种部署方案。支持在物理服务器和虚拟机上两种安装模式。 8. 系统中所有的内外部通讯接口均需采用安全通讯协议。如(SSH v2/TLS1.0/SSL3.0/IPSec/SFTP/SNMPv3 等） 9. 系统中所涉及的重要信息（如密码、Key）等信息均需要进行加密处理，不允许在系统的任何信息中出现明文记录。 10. 系统需要支持华为、Cisco、H3C、锐捷等主流厂商的设备管理能力。 11. 其他厂商设备的基础管理，系统需提供的快速自定义能力；高级管理厂商需提供定制开发，支持业务需要。 12. 系统需要支持路由器、交换机、防火墙、WLAN、服务器、存储、视频监

序号	货物名称	数量	技术参数及性能配置要求
			控、统一通信设备的统一管理和业务分析。厂商需提供官方网站链接及截图证明并加盖厂商有效印章； 13. 系统需要支持对管理对象（设备、端口）进行自定义分组能力。为了降低管理复杂度，系统需支持告警、性能、安全等策略自动应用到对应的分组，无须管理员进行多次配置。 14. 系统需要提供友好的图形化监控能力，能直观的展现出网络的拓扑。在拓扑界面上能够提供方便、快捷的操作（如：查看流量，性能，接入终端，区域划分等）及多方位的信息呈现。 15. 系统需支持拓扑拓扑节点的自定义能力，包括设备、链路等；可在拓扑上隐藏和去隐藏网络节点、并支持用户偏好设置能力。 16. 系统需要支持 7*24 小时对全网设备告警的实时监控，并支持多种远程通知能力（email、SMS），通知内容支持自定义。 17. 在告警信息中需要包含与故障关联的信息（如端口故障需关联呈现端口信息、故障信息、链路拓扑信息、历史流量信息、维护经验等）。 18. 支持基于任务的性能监控，7*24 监控网络性能。通过设置不同的性能阈值条件，可生成 4 级不同阈值告警：紧急、重要、次要、提示。支持历史性能的比较查看。 19. 可在性能管理界面中查看、编辑网管系统所有的性能监控的指标、采集周期等；性能监控需要支持用户习惯记忆功能，比如需要显示的列、列宽等，无需重复设置。 20. 性能管理需要支持灵活的分组方式和分组策略，新增的设备可自动按照规则进行自动的分组和监控，无须管理员手工创建性能监控任务。 21. 系统支持基于真实业务流的 IP 网络实时监测能力（非模拟报文监测或者探针式监测），监测结果可实时在拓扑上显示。 22. 系统提供的实时 IP 网络质量监测功能需要至少包含三个层次：设备级、链路级、网络级。 23. 系统支持丢包率的阈值告警能力，当系统监测到丢包率超过阈值后，可实时通知系统管理员。 24. 系统支持安全业务分析能力，支持安全策略配置、安全事件分析（提供 60 种以上安全事件分析类型），并支持提供图形、表格维度的报表功能；报表内容需要覆盖：DDoS 攻击报表、病毒报表、IPS 报表、上网行为报表、流量报表。 25. 系统支持全网安全事件分析功能、策略冗余分析和策略精简调优建议、提供设备策略健康度评估功能。 26. 系统提供常用的告警、性能、资源等报表查询；报表支持立即或者周期生成，可以通过 Email 发送；报表支持 excel、pdf、word 等形式的导出；支持忙时报表，忙时时间段支持用户自定义。 27. 系统提供报表自定义功能，通过在页面上拖拽快速生成报表，并提供多种数据展示和分析能力。 28. 具有软件著作权证书，提供复印件并加盖厂商公章或投标专用章。

序号	货物名称	数量	技术参数及性能配置要求
2	服务器	1 台	1. Intel Xeon 3106(8 核-1.7GHz-85W); 2. 可支持 2 颗 Intel Xeon Skylake 系列处理器； 3. 标配 1 条 DDR4 Registered DIMM 16GB; 4. 标配 2*GE+2*10GE 网口以太网卡； 5. 3008Raid 卡；600GB 硬盘， 6. 可支持配置 8 块 2.5inch 托架的 SATA/SAS 硬盘； 7. 可使用 PCIE raiser 卡扩展插槽； 8. N+1 个冗余系统风扇； 9. 4 个 USB（前面 2 个，后面 2 个）； 10. 集成 BMC 管理模块，板载华为 iBMC 管理模块，支持 IPMI、SOL、KVM Over IP、虚拟媒体等管理特性，对外提供 1 个 10/100Mbps RJ45 管理网口； 11. 支持 1+1 冗余电源， 12. 标配 2 个 550W 交流电源； 13. 无 DVD；导轨； 14. 2U 机架式
3	省局核心交换机	1 台	1. 交换容量≥15Tbps，包转发率≥1400Mpps 2. 主控引擎≥2；整机业务板槽位数≥3，支持颗粒化电源，整机电源槽位数≥3 3. 端口要求：1 块 48 端口十兆/百兆/千兆以太网电接口板;1 块 16 端口万兆以太网光接口和 16 端口千兆以太网光接口板；3 块千兆多模模块； 4. 颗粒化电源模块上支持电源开关，可控制单电源模块的供电状态，便于安装、维护及更换； 5. 支持 802.1X、MAC、Portal 等认证方式 6. 支持基于流量、DAA 目的地址和时长计费方式 7. 支持整机 MAC 地址≥1M;MAC 学习速率>8000/s,支持整机 ARP 表项≥256K;ARP 学习速率≥1000/s 8. 支持 4K VLAN，支持 1：1，N：1 VLAN mapping，端口 VLAN，协议 VLAN，IP 子网 VLAN；，Super VLAN;，Voice VLAN; 9. 支持 IEEE 802.1d(STP)、 802.w(RSTP)、 802.1s(MSTP) 10. 支持 1:1, N:1 端口镜像；流镜像；远程端口镜像（RSPAN）；ERSPAN，通过 GRE 隧道实现跨域远程镜像； 11. 支持 DHCP Client，DHCP Server，DHCP Relay；Option 82； 12. 支持 IPv4 路由转发 FIB 表项≥128K 13. 支持静态路由、RIP、RIPng、OSPF、OSPFv3、BGP、BGP4+、ISIS、ISISv6 14. 支持路由协议多实例，支持 GR for OSPF/IS-IS/BGP 15. 支持 IGMP Snooping V1,V2,V3；PIM-SM/DM/SSM；MLD V1，V2；IGMP Proxy； 16. 支持 IPv6 过渡技术，IPv4/IPv6 双栈、6over4 隧道、4 over6 隧道 17. 支持 IPv6 DHCP SERVER，IPv6 DHCP Relay，DHCP Snooping，支持 IPv6 Souce Guard 18. 支持 MPLS L3VPN、MPLS L2VPN(VPLS，VLL)、MPLS-TE、MPLS QoS 19. 支持整机 ACL 表项≥256K

序号	货物名称	数量	技术参数及性能配置要求
			20. 支持基于第二层、第三层和第四层的 ACL，双向 ACL；VLAN ACL 和 IPv6 ACL； 21. 支持 IP/Port/MAC 的绑定功能 22. 支持 PQ、WRR、DRR、PQ+WRR、PQ+DRR 调度方式；双向 CAR； 23. 提供广播风暴抑制功能；风暴控制支持 shutdown 端口或拒绝转发的安全策略下发； 24. 支持 WRED； 25. 支持 GE/10GE 端口 200ms 大缓存 26. 支持 5 级 H-QoS 27. 支持 DHCP Snooping trust，防止私设 DHCP 服务器； 28. 支持 DHCP snooping binding table (DAI, IP source guard)，防止 ARP 攻击、DDOS 攻击、中间人攻击； 29. 支持 BPDU guard， Root guard 30. 支持 802.1X、MAC、Portal 等认证方式 31. 支持真实业务流的实时检测技术，秒级快速故障定位 32. 支持 G.8032 标准环网协议 33. 支持 SNMP V1/V2/V3、Telnet、RMON、SSHV2 34. 支持通过命令行、中文图形化配置软件等方式进行配置和管理，WEB 网管 35. 为了提高网络的时钟精确性，需支持 1588v2 时钟功能 36. 支持能效以太网功能，IEEE 802.3az，提供第三方绿色节能认证证书 37. 通过 TUV 国际绿色产品认证，在环保、回收、节能、碳足迹等方面严格符合国际标准，并提供 TUV 绿色认证证书。 38. 通过 CC 认证，认证等级为 EAL3+，提供认证证书 39. 提供工信部入网证书
4	省局接入交换机	3 台	1. 交换容量≥336Gbps，包转发率≥108Mpps 2. 24 个千兆电口，4 个千兆 SFP；3 块千兆多模模块 3. 支持 MAC 地址≥8k，ARP 表项≥1K 4. 支持 4K 个 VLAN，支持 Voice VLAN，基于端口的 VLAN，基于 MAC 的 VLAN，基于协议的 VLAN，VLAN 内端口隔离 5. 支持 Smart link 6. 支持端口聚合，每个聚合组至少 8 个端口；支持跨设备链路聚合。 7. 支持 IGMP v1/v2/v3 Snooping 8. 支持 VLAN 内组播转发和组播多 VLAN 复制 9. 支持捆绑端口的组播负载分担 10. 支持可控组播，基于端口的组播流量统计 11. 支持防止 DOS、ARP 攻击功能、ICMP 防攻击，端口隔离、端口安全、Sticky MAC 12. 支持 DHCP Relay、DHCP Server、DHCP Snooping 支持 AAA 认证，支持 Radius、HWTACACS、NAC 等多种方式 13. 支持 CPU 保护功能，支持 CPU 攻击防范：支持 CPCAR，支持 CPU 队列限速 14. 支持基于第二层、第三层和第四层的 ACL 15. 支持 IP/Port/MAC 的绑定功能

序号	货物名称	数量	技术参数及性能配置要求
			16. 支持 G.8032 开放环网协议 17. 支持智能堆叠，堆叠后逻辑上虚拟为一台设备，具有统一的表项和管理，堆叠系统通过多台成员设备之间冗余备份 18. 支持以太网电口堆叠，用网线连接实现堆叠功能 19. 支持纵向虚拟化，作为纵向子节点零配置即插即用 20. 支持对端口接收报文速率和发送报文速率进行限制 21. 支持 SP、WRR、SP+WRR 等队列调度算法 22. 支持基于端口的流量监管 23. 支持基于队列限速和端口整形的功能 24. 支持 SNMP v1/v2/v3、Telnet、RMON 25. 支持通过命令行、Web、中文图形化配置软件等方式进行配置和管理，集群管理，带外管理以太网口； 26. 支持 802.3az 能效以太网 EEE，节能环保，提供权威第三方测试报告 27. 提供工信部入网证书
5	安装辅材	1 项	标签、跳线等

5.2、市县（林区）森林公安局

序号	货物名称	数量	技术参数及性能配置要求
1. 网络安全系统			
1	市县（林区）森林公安局出口下一代防火墙	24 台	1. 网络处理能力为 1G，并发连接≥20 万，每秒新建连接 2 万/秒， 桌面型设备，单电源，标准配置 4 个 10/100/1000M 自适应电口，1 个 Console 口；包括三年硬件维修服务。含三年入侵防御特征库升级服务、含三年病毒过滤特征库升级服务。含设备安装配置及调试服务。 2. 所投产品支持 MPLS 流量透传，并支持检测、防护 MPLS 流量中的安全威胁。 3. 所投产品必须支持 MTU≥9000byte 的巨型帧通过设备传输时不分段 4. 所投产品必须支持基于 IP、应用、服务的策略路由进行智能选路，支持源地址目的地址哈希、源地址哈希、时延负载、最优链路带宽负载、最优链路带宽备份、跳数等不少于 12 种路由负载均衡方式。 5. 所投产品必须支持不少于 8 条链路的 ISP 路由负载均衡，支持自定义链路负载权重，支持基于优先级的 ISP 路由链路备份；支持不少于 4 种的链路状态探测机制，实现失效链路快速切换 6. 所投产品支持 SNAT、DNAT。支持在源地址转换过程中，对 SNAT（源地址转换）使用的地址或地址池利用率进行监控，并在地址池利用率超过阈值时，通过 SNMPTrap、邮件、声音、短信等方式告警。 7. 所投产品必须支持基于源安全域、目的安全域、源用户、源地址、源地区、目的地址、目的地区、服务、应用、隧道、时间、VLAN 等多种方式进行访问控制，并支持地理区域对象的导入以及重复策略的检查。 8. 支持基于不同安全区域防御 DNSFlood、HTTPFlood 攻击，并支持警告、阻断、首包丢弃、TC 反弹技术、NS 重定向、自动重定向、手工确认等多种防护措施。

序号	货物名称	数量	技术参数及性能配置要求
			9. 所投产品应具备本地、云端双擎查杀能力，必须能够对HTTP/FTP/POP3/SMTP/IMAP/SMB六种协议进行病毒查杀，以及对至少6级压缩文件进行解压查杀 10. 所投产品必须支持针对FTP、HTTP、IMAP、OTHER_APP、POP3、SMB、SMTP等应用协议的漏洞攻击防护功能，至少可防御缓冲区溢出、跨站脚本、拒绝服务、恶意扫描、SQL注入、WEB攻击等类型的攻击 11. 所投产品应内置高质量漏洞攻击特征，应能够防御“永恒之蓝”、“震网三代”、“暗云3”、“Struts”、“Struts2”、“Xshell后门代码”等高危流行漏洞；漏洞特征应具备丰富的描述信息，至少包括对应的攻击的名称、CVEID、CNNVDID、严重性、影响的平台、类型、描述等详细信息 12. 所投产品支持配置虚系统，支持在虚系统内独立配置病毒防护、漏洞利用防护、间谍软件防护、URL过滤、文件过滤、内容过滤、邮件过滤、行为管控等安全功能。并可支持对本虚系统内产生的日志进行独立审计 13. 所投产品须提供关联的威胁事件日志，系统可自动将产生威胁事件的连接经过防病毒、防漏洞、防间谍软件、URL过滤、文件过滤等安全模块检查的日志集中显示，并支持对全部类型的日志模糊或精确检索。 14. 支持与云端联动，至少实现病毒云查杀、URL云识别、应用云识别、云沙箱、威胁情报云检测等功能 15. 具备公安部网络安全保卫局颁发的《计算机信息系统安全专用产品销售许可证》（增强级）（提供证明材料并加盖厂商公章） 16. 具备国家信息安全测评中心颁发的《信息技术产品安全测评证书》（EAL4+）（提供证明材料并加盖厂商公章） 17. 《中国国家信息安全产品认证证书》(提供证明材料并加盖厂商公章）
2	安装辅材	24项	标签、跳线等
2. 网络设备系统			
1	公安分局交换机	24套	1. 交换容量≥336Gbps，包转发率≥108Mpps 2. 为了提高设备可靠性，支持模块化可插拔双电源 3. 支持24个千兆电口，4个复用千兆光Combo口，4个万兆光口 4. 配置标准USB接口，支持U盘快速开局 5. 支持MAC地址规格≥16K，ARP表项规格≥4K 6. 支持4K个VLAN，支持Voice VLAN，基于端口的VLAN，基于MAC的VLAN，基于协议的VLAN，1:1和N:1 VLAN Mapping功能 7. 支持RIP、RIPng、OSPF、OSPFv3、ISIS、BGP等路由协议， 8. 支持Ipv4路由表≥8K，Ipv6路由表≥2K 9. 支持IPv4/IPv6双协议栈，支持6to4、ISATAP、手动配置tunnel 10. 支持DHCPv4/v6 client/relay/server 11. 支持三层IPv4组播路由协议PIM，三层IPv6组播路由协议MLD 12. 支持802.1x、MAC认证和Portal认证

序号	货物名称	数量	技术参数及性能配置要求
			13. 支持 DHCPv6 snooping、ND snooping、SAVI、MFF 14. 支持 CPU 保护功能 15. 支持 G.8032 开放环协议 16. 支持堆叠，主机堆叠数不小于 9 台 17. 支持以太网电口堆叠，用网线连接实现堆叠功能 18. 支持纵向虚拟化，作为纵向子节点零配置即插即用 19. 支持对端口接收报文速率和发送报文速率进行限制，支持 SP、WRR、SP+WRR 等队列调度算法 20. 支持 SNMP v1/v2/v3、Telnet、RMON、SSHv2； 21. 支持通过命令行、Web、中文图形化配置软件等方式进行配置和管理； 22. 支持零配置开局 23. 支持配置 NETCONF 作为云管理交换机 24. 支持能效以太网 EEE，节能环保，提供权威第三方测试报告 25. 提供工信部入网证书

5.3、森林公安派出所网络

序号	货物名称	数量	技术参数及性能配置要求
1	接入交换机	63 台	1. 交换容量 168Gbps，包转发率 41.66Mpps 2. 端口类型 24 个 10/100/1000Base-T 以太网端口，4 个千兆 SFP 3. 工作温度-5℃～50℃ 4. 防雷指标 7KV 5. 散热方式自然散热 6. MAC 表项 16K 7. VLAN 4K 8. 支持一键还原 9. 支持风暴抑制 10. 支持 U 盘开局 11. 支持 ACL 12. 支持 DHCP Snooping 13. 支持 STP 14. 支持 RSTP 15. 支持 MSTP 16. 支持 IPv6 17. 支持 CLI 18. 支持 IPv4/IPv6 静态路由 19. 支持 Voice Vlan
2	安装辅材	63 项	标签、跳线等

六、建设工期及运维要求

1、项目建设：中标人负责送货到采购人指定地点，并派技术人员免费施工、安装、调试、培训。

2、建设工期：合同签订之日起 90 天内

3、质保期：系统验收合格之日起，整个系统免费提供不少于三年的升级、维护服务

4、售后服务：投标人须有能力提供完善的售后服务（包括技术人员、响应时间等），中标人接到通知后 2 个小时内响应，8 个小时内派维修人员到达现场。