用 户 需 求 书

一、项目名称

海南省电子政务外网信息安全保障体系升级工程项目（项目编号：HNMY2018-049）

二、项目概述

2.1 概述

结合海南省电子政务外网建设现状，通过对安全威胁和实际需求的分析，遵照设计思路和设计原则，按照等级保护三级的基本要求进行总体规划和设计，为海南省电子政务外网的业务系统提供等保三级安全环境。

海南省电子政务外网数据中心安全框架从分层、纵深防御思想出发，根据层次分为物理安全、IT 基础架构安全（网络安全、主机安全）、虚拟化安全、数据安全、应用安全和安全管理等几个层面，结合云端安全服务用来指导海南省电子政务外网安全升级解决方案的设计。

2.2 项目建设目标及内容

2.2.1 项目建设目标

海南省政务外网是国家电子政务外网的重要组成，由海南省工业和信息化厅下属海南省党政信息中心具体负责建设和运维管理。海南电子政务外网是全省电子政务工作的重要载体，目前已经成为全省党政机关共用的电子政务基础设施，承载着处理大规模信息的任务。本次海南省电子政务外网改造项目的总体目标是通过建设安全资源，将海南省电子政务外网建设为等级保护三级安全防护能力，实现统一计算、存储、网络、安全管理和集中自动化运维服务，为各政务部门提供安全服务。

按照等级保护三级要求和海南省电子政务网络安全建设现状对海南省电子政务进行安全加固，建设高速、可靠、安全的电子政务网络，根据各网络的功能合理规划网络分区，满足相关法律法规要求，满足安全建设要求，为业务逐步迁移上云做好安全基础，并逐渐替换老旧热备。

2.2.2 项目建设内容

项目建设内容主要包括以下三大内容：

1、采用软件定义安全的架构构建安全防护体系

改造现有安全防护架构，采用软件定义安全的架构构建新电子政务云安全防护体系，建设具有面向各个信息系统的安全资源池，实现为各个业务系统提供独立可视的安全功能需求，满足不同部门个性化安全服务能力，实现安全按需扩展，弹性扩展，灵活部署。

2、升级部分安全产品

升级无法用安全资源池替代，并且过保、无法使用的、安全隐患较大的网络边界设备（老旧设备升级），加固原有安全防护。

3、新增安全设备

在安全管理区新加 2 堡垒机和 2 台数据库审计设备，运维管理区作为整个电子政务外网的管理运维“心脏”，进行云平台运维管理、安全设备的统一运维管理、数据库审计。

三、信息化基础设施现状

3.1 网络现状

网络分为三个区：互联网办公区、政务外网区、服务器对外发布区。互联网办公区用户访问政务网通过 inode 拨号认证通过后并切断互联网后才能访问政务外网；政务外网和对外发布区有数据交换需求时通过网闸进行数据摆渡。

互联网办公区：各单位的办公区，分为省委办公区、省政府办公室、海府办公室、互联单位，共用一个互联网出口，与政务外网区通过 inode 拨号认证互联，切断互联网后才能访问政务外网。

政务外网区：南北向和电子政务外网互联，承载核心内网业务，分为云平台、电子政务公共服务平台、RA 系统服务区、共享资源服务区等区域。未来电子政务公共服务平台、RA 系统服务区、共享资源服务区等的业务系统都会迁移到云平台上，对云平台进行统一防护和运维。

服务器对外发布区：承载对外发布的业务系统，有互联网出口，通过网闸和政务外网互联，未来业务系统也会向云端迁移。

3.2 安全设备

海南省电子政务外网使用的网络安全设备普遍运行了超过 5 年的时间，而且早已过了硬件质保的时间，若继续使用，将是网络安全运行的一个重大隐患。另

外，随着省电子政务外网上的业务应用增多，原有的一些关键部位使用的网络安全设备性能也不再能满足业务需求，而随着时间的迁移和硬件的更新换代，老旧的硬件无法兼容新的安全软件版本，这将导致现有的网络安全设备无法很好的防御新出现的网络威胁。因此，需要对这些老旧设备进行更新替换，以满足新安全软件版本对硬件的性能要求，同时避免设备老化带来的安全隐患。

而采用传统的方式对设备进行更新替换（采购新硬件对老硬件进行替换），有以下几点问题：

1、硬件替换，替换工作量庞大；

2、硬件替换，传统网络架构中的单点故障问题还是存在；

3、新硬件的维护量庞大；

4、5 年后新硬件依然面临着更新替换的需求，进入一个不良循环。

因此，我们建议使用安全资源池的形式，对老设备进行替换，不仅能减少更新替换的工作量和硬件的维护工作，而且基于超融合平台的安全资源池的性能可以进行弹性扩展，能满足未来 5-8 年的使用需求。当性能需要提高时，只需要对超融合平台进行性能扩展和提高安全资源池的性能资源分配，就能够平滑地实现安全性能的提升。

四、项目建设需求

4.1 概述

对电子政务外网的现有平台进行安全整改，主要包括政务外网和互联网区的安全资源池建设，互联网区的安全改造，将老旧设备逐渐替换，使用安全资源池的方式逐步替代，满足业务上云的安全需求。

项目建设内容主要包括以下三大内容：

1、采用软件定义安全的架构构建安全防护体系

改造现有安全防护架构，采用软件定义安全的架构构建新电子政务云安全防护体系，建设具有面向各个信息系统的安全资源池，实现为各个业务系统提供独立可视的安全功能需求，满足不同部门个性化安全服务能力，实现安全按需扩展，弹性扩展，灵活部署。

2、升级部分安全产品

升级无法用安全资源池替代，并且过保、无法使用的、安全隐患较大的网络

边界设备（老旧设备升级），加固原有安全防护。

3、新增安全设备

在安全管理区新加 2 堡垒机和 2 台数据库审计设备，运维管理区作为整个电子政务外网的管理运维“心脏”，进行云平台运维管理、安全设备的统一运维管理、数据库审计。

4.2 规划升级范围

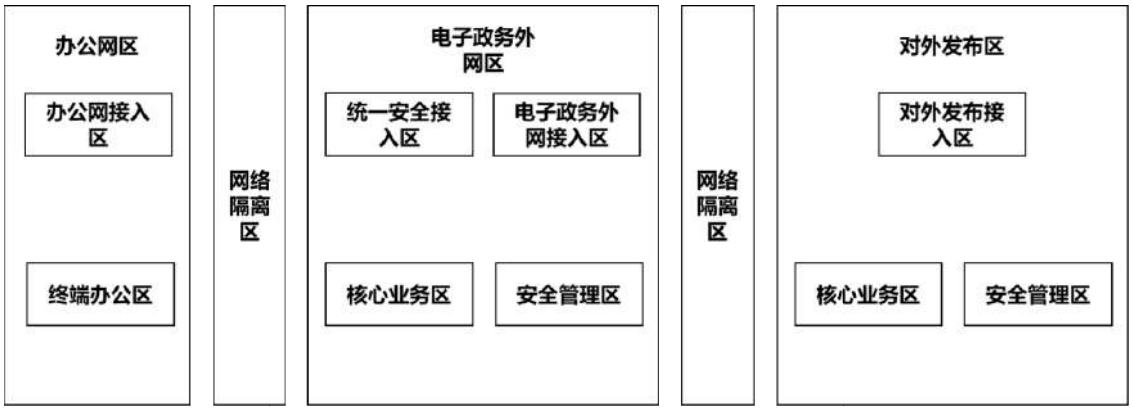

图 3-1 海南省政府电子政务网新全网拓扑示意图

4.3 安全域划分

海南省党政信息中心电子政务外网共分为三个网络分区：办公网区、电子政务外网区、对外发布区。

安全域的划分是安全体系构建的基础，事实上每一个安全边界所包含的区域都形成了一个安全域。这些区域具有不同的使命，具有不同的功能，分域保护的框架为明确各个域的安全等级奠定了基础，保证了信息流在交换过程中的安全性。

建设方案需严格按照电子政务外网相关标准，以及信息系统的重要性和网络使用的逻辑特性划分安全域，包括但不限于如下安全域：

1）网络接入区，该区域说明如下：将承载电子政务外网接入、互联网接入、统一安全接入的职责，细分为电子政务外网接入区、对外发布接入区、办公接入区、统一安全接入区，四个安全区域；

2）网络隔离区，该区域说明如下：在电子政务外网区、办公网区、对外发布区三个网络的边界用必要的技术手段进行安全隔离；

3）核心业务区，该区域说明如下：该区域主要承载租户业务系统的系统运转；根据业务系统的不同可以细分为政务外网业务服务区、对外发布业务服务区两个细分区域，承担对应职责；

4）运维管理区，该区域说明如下：该区域主要承载针对整体网络的统一安全管理、病毒库统一升级、SDN 管理等服务，按照要求本区域不与业务网络掺杂，应单独构建管理运维网络。

四、项目清单

投标人必须按照项目初步设计概算汇总表清单（下表）进行报价；投标人应充分考虑项目所需要的辅助材料，如工程量清单中未列出或数量不足，投标人应给予补充，并计入投标总报价中。

主要设备功能需求、技术指标要求详见前面描述，投标人必须点对点响应，否则视为不满足。

1.硬件设备：

序号	分项名称	性能指标	数量	单位	备注
1、安全设备					
1	下一代防火墙	要求详见“五、核心产品技术指标”	2	台	
2	数据库审计	要求详见“五、核心产品技术指标”	2	台	
3	堡垒机	要求详见“五、核心产品技术指标”	2	台	
4	网闸	要求详见“五、核心产品技术指标”	2	台	
2、服务器与存储设备					
1	服务器	要求详见“五、核心产品技术指标”	4	台	

2.软件产品：

序号	分项名称	性能指标		数量	单位	备注

1、互联网区安全软件						
1	安全资源池	基本配置： 安全资源池软件永久授权 包括基础防火墙功能授权，IPS 模块授权，AV 模块授权，WAF 模块授权，以上每种安全能力至少支持 10 个安全域的部署，单个安全组件至少支持 10Gbps 三层吞吐，至少支持 2Gbps 应用层吞吐。整个软件平台最大支持扩容至 20Gbps 应用层吞吐。 包含： 安全资源池 URL 库许可及特征库升级服务 3 年 IPS 模块特征库升级服务 3 年 AV、WAF 模块特征库升级服务 3 年 网站安全防护包及 3 年升级服务 **要求详见“五、核心产品技术指标”**		1	套	
2、电子政务外网区安全软件						
2	安全资源池	基本配置： 安全资源池软件永久授权 包括基础防火墙功能授权，IPS 模块授权，AV 模块授权，WAF 模块授权，以上每种安全能力至少支持 10 个安全域的部署，单个安全组件至少支持 10Gbps 三层吞吐，至少支持 2Gbps 应用层吞吐。整个软件平台最大支持扩容至 20Gbps 应用层吞吐。 包含： 安全资源池 URL 库许可及特征库升级服务 3 年 IPS 模块特征库免费升级服务 3 年 AV、WAF 模块特征库免费升级服务 3 年 **要求详见“五、核心产品技术指标”**		1	套	

五、核心产品技术指标

设备名称	技术指标	数量
1、安全设备		
下一代防火墙	1. 整机吞吐量　≥10Gb； 2. 应用层吞吐量　≥2Gb； 3. 并发连接数　≥220 万； 4. 每秒新建连接数　≥13 万； 5. ▲设备接口　标配≥6 个千兆电口，≥4 个千兆光口，≥2 个万兆 SFP+口及模块,≥2 个通用业务扩展插槽； 6. 电源：冗余电源； 7. 支持透明、路由、混合、旁路 4 种工作模式； 8. 支持源 NAT 和目的 NAT,且支持 NAT 扩展技术，使单个公网 IP 支持的 NAT 转换端口突破 65535 限制； 9. 支持 OSPF、BGP、RIPv1/v2、IS-IS（动态路由协议非透传）路由； 10. 策略路由：支持基于应用引流技术，提供基于时间、应用协议的策略引流，如针对 P2P、WEB 视频协议，通过深度应用识别，将这些应用产生的流量引流到特定的互联网线路上；支持基于 URL 引流技术，支持基于时间、URL 的智能引流技术，通过 DPI 的智能引流技术，从而对具体 URL 的访问动作进行策略引流，将某个 URL 的流量引到特定的链路上； 11. 支持根据国家/地区来进行地域访问控制； 12. 支持策略冗余检测，对策略重复检查； 13. 设备具备独立的入侵防护漏洞规则特征库； 14. 支持对网站黑链进行检测； 15. 支持场景化的配置向导功能，可以选择不同的部署方式以及使用场景实现产品的快速实施； 16. 抗 DDOS 攻击：支持抵御下所列所有攻击类型，包括：DNS Query Flood、SYN Flood、UDP Flood、ICMP Flood、Ping of Death、Smurf、WinNuke； 17. 支持 ALG 应用，包括：H.323、SIP、FTP、TFTP、RSH、RTSP、	2

	SQL Net、HTTP、MS-RPC、PPTP/GRE、SUN-RPC 18. 智能流量管理：支持管道嵌套，能够同时做到多个维度的流量控制；支持对多层级管道进行最大带宽限制、最小带宽保证、每 IP 或每用户的最大带宽限制和最小带宽保证； 19. 所提供的设备必须支持 IPV6、IPV4 双栈接入； 20. 提供安全运维 APP：通过手机可以第一时间获知设备的实时 CPU、内存、流量趋势，以及应用、用户排名、威胁信息等安全状态、 帮助快速定位问题、安全可视化实时呈现，该 APP 不限制使用用户数； 21. 提供所用的全部功能组件三年的病毒库升级、特征库升级、软件升级、硬件质保等相关升级费用，并提供三年售后服务（包含策略调整服务）。 资质要求： 1. 投标产品具备公安部颁发的《计算机信息系统安全专用产品销售许可证》； 2. 投标产品具备中国信息安全认证中心颁发的《中国国家信息安全产品认证证书》万兆 3. 投标产品必须提供信息技术产品安全测评证书（EAL3+）； **4.** 投标产品具备国家版权局颁发的《计算机软件著作权登记证书》,包括具有自主知识产权的 64 位安全操作系统、多核并行操作系统、QoS 流量管理、攻击防护、病毒过滤、入侵防御等证书；	
数据库审计	1. 系统：MTBF(平均故障间隔时间)≥65000 小时； 2. 处理器：采用当前主流 Intel 酷睿第四代 I7 系列 CPU，主频至少 3.4G，至少 4 核 8 线程； 3. 内存：≥16GB DDR3 1600Mhz； 4. 电源模块：具备冗余热插拔双电源；冗余热插拔风扇； 5. 硬盘可用容量：≥2TB，支持 RAID0， RAID5 阵列，最大支持扩展到 4T*4； 6. ▲支持千兆网络环境下的监听能力，配备至少 2 个千兆电口管理口；至少 4 个千兆业务电口，至少 4 个千兆业务光口； 7. ▲审计性能：能够稳定、流畅地同时支持 16 个以上数据库审计能力，不会产生漏审； 8. 吞吐能力：≥4000M，日处理业务操作数：≥4 亿条；峰值处理能力：≥6 万条/秒；	2

	9．审计日志检索能力：≥3000 万条/秒； 10．支持 Oracle、SQL-Server、DB2、Informix、Sybase、MySQL 等主流数据库审计； 11．支持主流业务协议 HTTP、Telnet、FTP、SMTP、POP3、DCOM； 12．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； 13．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； 14．支持通过部署 agent 实现 java web 环境 100%准确关联 15．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 16．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；； 17．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； 18．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； 19．支持 IPV6、IPV4 双栈接入； 20．提供不少于三年产品原厂商特征库、软件升级和硬件质保服务（包含策略调整服务）。 资质要求： 1．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》。	
堡垒机	1．要求采用物理旁路模式部署，不影响网络结构。 2．要求系统为 B/S 架构，采用 HTTPS 方式远程安全管理，无需安装客户端。 3．▲要求含交流双电源模块，≥2*USB 接口，≥1*RJ45 串口，≥1*GE 管理口，≥6*GE 电口，≥1 个接口扩展槽，≥2T SATA 硬盘，管理设备数≥200 台，最大可支持管理 2000 台。图形会话并发不少于 600 个，字符会话并发不少于 800 个。 4．▲要求支持字符型远程操作协议：SSH（V1、V2）、TELNET；支持图形化远程操作协议：RDP、VNC、X11；支持文件传输协议:FTP、TFTP； 5．要求可通过应用发布的方式进行协议扩展，无需定制即可支	2

	持其他通用及专有的运维客户端程序。 6. 要求支持 HTTP、HTTPS 操作审计，HTTP/HTTPS 协议可以直接代理。 7. 能够提供对各从账号的运维使用率的分析功能，当发现使用率异常的从账号，对相关管理员采取告警、记录及通知等操作。 8. 产品须获得中国信息安全测评中心颁发的《信息技术产品安全测评证书》EAL3+级别， 9. 产品须具备公安部颁发的《计算机信息系统安全专用产品销售许可证》 10. 所提供的设备须支持 IPV6、IPV4 双栈接入； 11. 提供不少于三年产品原厂商特征库、软件升级和硬件质保服务（包含策略调整服务）。	
网闸	1. ▲不少于 12 个 10/100/1000M 自适应电口，2 个万兆光接口和模块；内外网主机系统分别具有独立的网络口、管理口、HA 口（热备口）、USB 口； 2. 设备提供实时显示设备工作状态及配置信息。 3. 双冗余电源；系统吞吐量≥9Gbps；并发连接数≥60 万； 4. 支持病毒检测、文件交换、数据库同步、数据库访问、安全浏览、FTP 访问、邮件传输、定制访问、二次开发、流媒体传输等基本功能； 5. 内、外网主机系统分别采用冗余双系统启动模式，当 A 系统运行失败后，能从 B 系统启动，且 A、B 系统可互为备份； 6. 主机系统具有自主知识产权的多核多线程 ASIC 并行操作系统平台； 7. 支持 IPV6、IPV4 双栈接入； 8. 支持有客户端无客户端两种文件交换方式；支持完全复制、增量同步、发送后删除、发送后备份等多种同步策略；支持多线程处理任务； 9. 支持断点续传；支持对文件名关键字过滤，支持文件大小限制，支持时间策略； 10. 支持支持 oracle、Sql Server 、DB2、Sybase、MySQL 等主流数据库间的同种或异种数据库同步，支持单向和双向同步； 11. 支持数据容错处理，当数据同步失败时，用户可以查询、复位、删除未能正常传输的数据； 12. 支持 HTTP 请求类型（GET/POST/PUT/HEAD）过滤；支持 HTTP	2

	请求头部大小限制； 13. 支持文件类型（文件扩展名）过滤；MIME 类型过滤；支持时间策略 14. 实现安全的 FTP 访问，支持对访问用户、访问协议命令、上传下载文件类型等进行过滤控制； 15. 提供专用客户端，与网闸进行认证，支持本地用户名口令认证，支持对在线用户进行踢除、中断、查看等管理方式； 16. 具有实时入侵检测机制，实时阻断入侵； 17. 具有抗 DoS、DDoS 攻击功能； 18. 支持病毒检测功能； 19. 管理方式采用 B/S 架构的 Web 方式管理，基于数字证书管理； 20. 支持全中文日志显示；支持 FTP 方式远程存储日志；支持日志按模块查询； 21. 双机热备支持配置同步；支持负载均衡； 22. 支持图表实时显示网口流量、CPU 状态、内存状态信息； 23. 所提供的设备须支持 IPV6、IPV4 双栈接入； 24. 具备公安部《计算机信息系统安全专用产品销售许可证》（万兆）； 25. 国家信息安全测评信息技术产品安全测评证书（EAL3 万兆 IPV6）； 26. 符合环保节能要求，入围工信部节能目录； 27. 提供不少于三年产品原厂商特征库、软件升级和硬件质保服务（包含策略调整服务）。	
2、服务器与存储设备		
服务器	1. ▲支持≥2 颗英特尔至强可扩展系列处理器，本次配置 2 颗处理器，单处理器主频≥2.2GHz，≥14 核，三级缓存≥19.25M； 2. 内存类型：ECC DDR4 2400MHz 或以上 RDIMM 内存插槽，内存槽位最大支持≥24 个； 3. ▲配置 4 根 32GB DDR4 内存，共 128GB 内存容量；内存保护支持 ECC、内存镜像、SDDC、内存热备、Lockstep； 4. ▲配置 1 块 240GB SSD 硬盘，1 块 480GB SSD 硬盘和 1 块 4TB SATA 硬盘，支持热插拔 SAS/SATA/SSD 硬盘； 5. ▲配置磁盘阵列卡，支持 RAID0,1,5,6,10,50,60，1GB 缓存，提供超级电容掉电保护； 6. ▲本次配置 6 个千兆网口和 2 个万兆光口；	2

	7. 长期工作环境温度支持 5-45 度； 8. 配置交流双电源，提供配套的电源连接线；满配冗余风扇，支持单风扇失效； 9. 可管理和维护性:1. 集成系统管理处理器支持：自动服务器重启、风扇监视和控制、电源监控、温度监控、启动/关闭、按序重启、本地固件更新、错误日志，可通过可视化工具提供系统未来状况的可视显示； 2.具有图形管理界面及其他高级管理功能，； 10. 支持 Windows，SLES，RHEL 操作系统；支持 Vmware，Citrix 虚拟化软件。 11. 所有配件提供不少于三年产品原厂商质保服务。	

软件设备名称	**技术指标**	**数量**
安全资源池	1. ▲本次至少提供的虚拟化安全组件的安全能力至少包括传统防火墙、IPS、WAF、防病毒网关,以上每种安全能力至少支持 10 个安全域的部署； 2. ▲能够识别管控的应用类型超过 1200 种，应用识别规则总数超过 3000 条；内置病毒样本数量超过 200 万；具备独立的入侵防护漏洞规则特征库，特征总数在 7000 条以上；具备独立的僵尸网络识别库，特征总数在 40 万条以上；具备独立的 WEB 应用防护识别库，特征总数在 3000 条以上； 3. ▲单个安全组件至少支持 10Gbps 三层吞吐,至少支持2Gbps应用层吞吐,整个软件平台最大支持扩容至 20Gbps 应用层吞吐； 4. 为保障平台的扩展性和兼容性，方便后续扩容，平台的计算资源、存储资源、网络资源、网络功能资源、安全功能等 IT 基础资源必须虚拟化； 5. 资源池必须具备安全需求弹性扩展能力，其中可扩展的安全功能中必须包含：虚拟应用负载均衡、虚拟下一代防火墙、虚拟数据库审计、虚拟上网行为管理、虚拟日志审计、虚拟堡垒机、终端检测响应等功能组件； 6. 基于 X86 服务器平台部署，可支持透明、路由、混合、旁路 4 种工作模式，可以通过 SDN、策略路由实现流量牵引； 7. 支持源 NAT 和目的 NAT,且支持 NAT 扩展技术，使单个公网	2

	IP 支持的 NAT 转换端口突破 65535 限制； 8. 支持 OSPF、BGP、RIPv1/v2、IS-IS（动态路由协议非透传）路由； 9. 策略路由：支持基于应用引流技术，提供基于时间、应用协议的策略引流，如针对 P2P、WEB 视频协议，通过深度应用识别，将这些应用产生的流量引流到特定的互联网线路上；支持基于 URL 引流技术，支持基于时间、URL 的智能引流技术，通过 DPI 的智能引流技术，从而对具体 URL 的访问动作进行策略引流，将某个 URL 的流量引到特定的链路上； 10. 抗 DDOS 攻击：支持抵御下所列所有攻击类型，包括：DNS Query Flood、SYN Flood、UDP Flood、ICMP Flood、Ping of Death、Smurf、WinNuke； 11. 支持 ALG 应用，包括：H.323、SIP、FTP、TFTP、RSH、RTSP、SQL Net、HTTP、MS-RPC、PPTP/GRE、SUN-RPC 12. 能够实现对安全的自助可控服务，必须具备独立的可视化界面，可查看：当前虚拟安全架构图安全资源运行状态、安全状态，可配置：当前的安全资源，如下一代防火墙、数据库审计等安全功能的策略管控。 13. 平台支持关键安全组件双机功能，保障安全组件高可用 14. 支持虚拟机卡死及蓝屏的检测功能并实现自动重启，无需人工干预减少运维工作量； 15. 可以通过设置对集群服务器基础资源根据资源负载状态动态调度不同集群服务器的 CPU、内存等资源； 16. 支持针对网站的漏洞扫描进行防护，能够拦截漏洞扫描设备或软件对网站漏洞的扫描探测 17. 具备支持终端安全端点探针实时安全威胁感知能力，通过基于威胁情报和行为分析日志的统计检测能力实现对恶意 IP 实时封堵； 18. 支持对检测到的攻击行为按照 IP 地址的地理位置信息进行威胁信息动态展示，实时监测和展示最新的攻击威胁信息； 19. 支持自动生成安全风险报表，报表内容体现被保护对象的整体安全等级，发现漏洞情况以及遭受到攻击的漏洞统计，具备有效攻击行为次数统计和攻击举证； 20. 支持对终端已被种植了远控木马或者病毒等恶意软件进行检测，并且能够对检测到的恶意软件行为进行深入的分析，展	

	示和外部命令控制服务器的交互行为和其他可疑行为； 21. 支持 Web 漏洞扫描功能，可扫描检测网站是否存在 SQL 注入、XSS、跨站脚本、目录遍历、文件包含、命令执行等脚本漏洞； 22. 提供所用的全部功能组件三年的病毒库升级、特征库升级、软件升级等相关升级费用，并提供三年售后服务（包含策略调整服务）； 23. 所投产品必须提供具备《计算机软件著作权》； 24. 所投产品必须提供《计算机信息系统安全专用产品销售许可证》； 25. 所提供的安全组件须支持 IPV6、IPV4 双栈接入。	

2、项目交货期

自合同签订之日起 60 天内招标人指定地点

3、售后服务

（1）服务期限。除已约定外，对整体系统、设备、软件均提供为期不少于 2 年的整体免费质保。

（2）必须配合采购人对安全策略进行迁移和调整工作。

（3）质保配件保障。质保期内，如配件出现故障无法修复，供应商负责免费更换或提供同等技术参数的替代品。

（4）质保服务方式。上门服务，提供 5×8 小时上门保修，7×24 小时技术支持和服务。

（5）质保服务响应效率。2 小时内作出实质性响应，4 个小时内到达现场，12 个小时内解决问题。

4、其他

1、如中标人的报价过低（低于预算金额的 80%），则采购人有权要求中标人提供中标金额的 10%作为履约银行保函，同时预付款比例调整为 0%。如中标人在实施过程中未按招标文件和合同要求实施，超过工期等行为，则采购人有权终止合同，并报主管部门严肃处理。

2、投标人的报价明显低于其他通过符合性审查投标人的报价，有可能影响产品质量或者不能诚信履约的，要求其在评标现场合理的时间内提供书面说明，必要时提交相关证明材料；投标人不能证明其报价合理性的，将其作为无效投标处理。

3、投标人所投产品技术指标应答必须真实有效，若发现虚假应答、不能满足采购人需求的，采购人有权要求更换为合格设备甚至终止合同，并报主管部门严肃处理。