附件1

百色市人民医院网络安全防护升级参数

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **项号** | **货物名称** | **数量** | **单位** | **技术参数** |
| 1 | 专网防火墙续保授权 | 1 | 项 | 1. 提供采购人在用的防火墙系统应用识别库、URL分类特征库、病毒防护特征库、入侵防御特征库升级服务及威胁情报订阅服务三年授权许可，续保授权须与原系统品牌一致，系统原有功能及模块须予以保留。
 |
| 2 | 互联网出口防火墙续保授权 | 1 | 项 | 1. 提供采购人在用的防火墙系统应用识别库、URL分类特征库、病毒防护特征库、入侵防御特征库升级服务及威胁情报订阅服务三年授权许可，续保授权须与原系统品牌一致，系统原有功能及模块须予以保留。
 |
| 3 | 态势感知平台授权 | 1 | 项 | 1. 提供采购人在用的态势感知平台三年威胁情报更新及规则库升级授权许可，续保授权须与原系统品牌一致，系统原有功能及模块须予以保留。
 |
| 4 | 服务器区防火墙 | 2 | 台 | 1. 标准2U设备，冗余电源；配置≥8个10/100/1000M自适应电口，8个SFP插槽，6个SFP+插槽，另有2个接口板卡扩展插槽，4TB机械硬盘，1个Console口，配置液晶屏，含三年硬件质保和应用识别库、URL分类特征库、病毒防护特征库、入侵防御特征库升级服务及威胁情报订阅服务。
2. 防火墙吞吐≥40Gbps，并发连接数≥1200万，每秒新建连接数≥40万/秒，包含应用控制、URL过滤、病毒防护、入侵防御、威胁情报检测等功能模块。
3. 支持MPLS流量透传；支持针对MPLS流量的安全审查，包括漏洞防护、反病毒、间谍软件防护、内容过滤、URL过滤、基于终端状态访问控制等安全防护功能。
4. 支持基于策略的路由负载，支持根据应用和服务进行智能选路，支持源地址目的地址哈希、源地址哈希、轮询、时延负载、备份、随机、流量均衡、源地址轮询、目的地址哈希、最优链路带宽负载、最优链路带宽备份、跳数负载等不少于12种路由负载均衡方式。
5. 支持在源地址转换过程中，对SNAT（源地址转换）使用的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SNMP Trap、邮件等方式告警。
6. 支持DDNS功能，支持Oray向日葵、Pubyun公云、Noip、Changeip提供的DDNS服务，将动态获取的IP地址映射为固定的域名。
7. 支持DS-Lite CPE B4功能，支持成为b4或aftr角色，支持从DHCPv6服务器或手动方式获取AFTR参数。
8. 支持在虚拟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。
9. 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。
10. 支持共享上网检测功能，可以通过设置管控地址和例外地址优化管控功能，同时支持阻断或告警动作。
11. 支持将其他硬件安全设备（包括但不限于防火墙、IPS、IDS、WAF、行为管理、流量探针等）加入网元组，并接受流量编排；支持将同类型安全设备划归同一网元组，组成硬件安全资源池（如WAF安全资源池），并将流量通过负载均衡（“源地址哈希”、“源目的地址哈希”，“加权源地址哈希”、“加权源目的地址哈希”、“加权地址端口哈希”、“轮询”和“权重轮询”）的方法编排给组内所有网元。
12. 支持灵活的服务链编排功能，支持串接链和旁路链，支持网元组的方向和位置设置。
13. 支持灵活的细粒度引流策略，可基于源安全域、目的安全域、源用户、源地址、目的地址、服务、VLAN、服务链、流量方向（内网到外网/外网到内网）的引流策略，并详细记录日志。
14. 支持对编排的流量进行监控，至少能从网元组、引流策略两个维度对编排流量监控统计。
15. 支持基于不同安全区域防御SYN Flood、UDP Flood、ICMP Flood、IP Flood、DNS Flood、HTTP Flood、NTP Query Flood 、NTP Reply Flood 和SIP Flood 攻击，并支持警告、丢弃、普通防护（首包丢弃）、增强防护（TC反弹技术）、授权服务器防护（NS重定向）、普通防护（自动重定向）、增强防护（手工确认）等多种防护措施。
16. 支持DHCP协议防护；支持手动定义可信DHCP服务器IPv4和基于阈值限制DHCP请求传输速率。
17. 支持IPv4和IPv6流量的HTTPS、POP3S、SMTPS、IMAPS协议进行解密，支持配置基于源安全域、目的安全域、源地址、目的地址、SSL协议服务的解密策略，动作可以设置解密或不解密。
18. 支持IPv4和IPv6流量的蜜罐引流策略，支持配置基于源安全域、目的安全域、源地址、目的地址、服务、VLAN的引流策略，并支持强制导流，能够通过设置服务器和端口进行引流。
19. 支持作为轻量级“探针”与采购人在用的的态势感知平台联动，上报网络活动产生的数据至态势感知平台；并支持接收来自态势感知平台推送的处置策略，及时拦截绕过防御措施产生的高级威胁。
20. 支持与本项目中的终端安全管理系统联动，实现基于终端健康状态的访问控制；并支持阻断“高风险”终端网络活动的同时，提示被阻断原因及重定向自定义网址。
 |
| 5 | 安全管理区防火墙 | 1 | 台 | 1. 标准1U设备，单电源；配置≥8个10/100/1000M自适应电口，2个SFP插槽，2个SFP+插槽，另有2个接口板卡扩展插槽，1TB机械硬盘，1个Console口，含三年硬件质保和应用识别库、URL分类特征库、病毒防护特征库、入侵防御特征库升级服务及威胁情报订阅服务。
2. 防火墙吞吐≥8Gbps，并发连接数≥200万，每秒新建连接数≥10万/秒，包含应用控制、URL过滤、病毒防护、入侵防御、威胁情报检测等功能模块。
3. 支持MPLS流量透传；支持针对MPLS流量的安全审查，包括漏洞防护、反病毒、间谍软件防护、内容过滤、URL过滤、基于终端状态访问控制等安全防护功能。
4. 支持基于策略的路由负载，支持根据应用和服务进行智能选路，支持源地址目的地址哈希、源地址哈希、轮询、时延负载、备份、随机、流量均衡、源地址轮询、目的地址哈希、最优链路带宽负载、最优链路带宽备份、跳数负载等不少于12种路由负载均衡方式。
5. 支持在源地址转换过程中，对SNAT（源地址转换）使用的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SNMP Trap、邮件等方式告警。
6. 支持DDNS功能，支持Oray向日葵、Pubyun公云、Noip、Changeip提供的DDNS服务，将动态获取的IP地址映射为固定的域名。
7. 支持DS-Lite CPE B4功能，支持成为b4或aftr角色，支持从DHCPv6服务器或手动方式获取AFTR参数。
8. 支持在虚拟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。
9. 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。
10. 支持共享上网检测功能，可以通过设置管控地址和例外地址优化管控功能，同时支持阻断或告警动作。
11. 支持将其他硬件安全设备（包括但不限于防火墙、IPS、IDS、WAF、行为管理、流量探针等）加入网元组，并接受流量编排；支持将同类型安全设备划归同一网元组，组成硬件安全资源池（如WAF安全资源池），并将流量通过负载均衡（“源地址哈希”、“源目的地址哈希”，“加权源地址哈希”、“加权源目的地址哈希”、“加权地址端口哈希”、“轮询”和“权重轮询”）的方法编排给组内所有网元。
12. 支持灵活的服务链编排功能，支持串接链和旁路链，支持网元组的方向和位置设置。
13. 支持灵活的细粒度引流策略，可基于源安全域、目的安全域、源用户、源地址、目的地址、服务、VLAN、服务链、流量方向（内网到外网/外网到内网）的引流策略，并详细记录日志。
14. 支持对编排的流量进行监控，至少能从网元组、引流策略两个维度对编排流量监控统计。
15. 支持基于不同安全区域防御SYN Flood、UDP Flood、ICMP Flood、IP Flood、DNS Flood、HTTP Flood、NTP Query Flood 、NTP Reply Flood 和SIP Flood 攻击，并支持警告、丢弃、普通防护（首包丢弃）、增强防护（TC反弹技术）、授权服务器防护（NS重定向）、普通防护（自动重定向）、增强防护（手工确认）等多种防护措施。
16. 支持DHCP协议防护；支持手动定义可信DHCP服务器IPv4和基于阈值限制DHCP请求传输速率。
17. 支持IPv4和IPv6流量的HTTPS、POP3S、SMTPS、IMAPS协议进行解密，支持配置基于源安全域、目的安全域、源地址、目的地址、SSL协议服务的解密策略，动作可以设置解密或不解密。
18. 支持IPv4和IPv6流量的蜜罐引流策略，支持配置基于源安全域、目的安全域、源地址、目的地址、服务、VLAN的引流策略，并支持强制导流，能够通过设置服务器和端口进行引流。
19. 支持作为轻量级“探针”与采购人在用的的态势感知平台联动，上报网络活动产生的数据至态势感知平台；并支持接收来自态势感知平台推送的处置策略，及时拦截绕过防御措施产生的高级威胁。
20. 支持与本项目中的终端安全管理系统联动，实现基于终端健康状态的访问控制；并支持阻断“高风险”终端网络活动的同时，提示被阻断原因及重定向自定义网址。
 |
| 6 | 入侵防御系统 | 2 | 台 | 1. 2U机箱，冗余电源；配置≥8个10/100/1000M自适应电口，8个千兆SFP插槽，6个万兆SFP+插槽，2个扩展插槽，1个Console口，2个USB接口，4T机械硬盘；配置液晶屏，提供三年硬件维保、入侵防御特征库升级、应用识别库升级和威胁情报订阅服务。
2. 网络层吞吐≥40Gbps，入侵防御吞吐≥6Gbps，并发链接≥800万，新建速率≥20万/秒。
3. 产品支持路由、旁路、交换以及混合模式接入。
4. 支持基于IPv4或IPv6的TCP、HTTP、DNS、ICMP、Radius方式的链路探测联动，同时TCP与HTTP可使用自定义目标端口进行测试；支持BFD联动。
5. 支持IPv4和IPv6的静态DNS功能，即从指定的入接口或源ISP接收到的DNS解析请求，设备可根据自定义的域名和IP对应关系，代理DNS服务器返回查询结果。
6. 支持4in6隧道过渡技术，至少包含DS-Lite协议中的b4和aftr能力，以及支持从DHCPv6服务器或手动方式获取AFTR参数。
7. 支持命中时间分析和安全策略推荐，命中时间分析展示被命中的安全策略的名称、状态、命中数、策略创建时间、首次命中时间和最近命中时间；安全策略推荐定可以指定策略流量，分析后自动生成源地址精度更高的安全策略。
8. 支持应用识别，应用特征库包含的应用数量（非应用协议的规则总数）大于3000种，可深度识别每种应用的属性，为每种应用提供预定义的风险系数，并将应用基于类型、数据传输、风险等级等特征分类。
9. 支持对应用的文件传输行为进行上传、下载、双向的文件类型过滤，应用至少包含即时通讯、常用协议、文件共享、论坛、博客、网页邮件、微博七种分类。
10. 支持基于Flood攻击和恶意扫描的的流量自学习能力，可自定义开始时间、学习时长、查看学习结果，并根据学习结果一键生成DDOS防护策略。
11. 支持RA管控策略， 用于防止RA攻击。支持基于源MAC、SSLA MAC、源地址、VLAN、前缀、跳数等条件进行RA管控。能够基于M标记、O标记进行置位和不置位检测管控。
12. 支持弱口令检测，支持主动检测和被动检测两种检测方式；支持基于网段、协议、用户名字典、弱口令字典进行完整扫描，执行方式包含手动和自动；能够基于数字、字母、数字和字母、自然顺序、键盘顺序、特殊字符、用户名、重复字符等进行弱口令检测。
13. 支持暴力破解能力，至少支持FTP、IMAP、WEBLOGIC、VNC、Telnet、RLOGIN、RDP等14种协议，且可手动设置攻击频率、持续检测时间，并支持日志、阻断、放行、重置和加入动态黑名单的处置动作。
14. 支持自定义TCP、UDP、HTTP协议的漏洞特征，漏洞特征可通过多个字段以文本或正则表达式的形式进行有序和无序匹配，并可自定义漏洞的源、目的端口范围；同时可标识自定义漏洞的CVE编号或CNNVD编号。
 |
| 7 | Web应用防火墙 | 1 | 台 | 1. 标准2U机箱，冗余电源，具有液晶面板，1TB硬盘。配置≥4个千兆10/100/1000M自适应电口，≥4个千兆SFP插槽，≥2个万兆SFP+插槽，1个Console口，2个USB口，另有1个扩展插槽。支持Web安全保护≥512个站点。含三年WAF软件特征库服务及硬件质保服务。
2. 网络吞吐量≥10Gbps，应用层处理能力≥6Gbps，网络并发连接数≥400万，HTTP并发≥150万，HTTP新建连接数≥60000/s。
3. 支持在旁路镜像阻断模式下，可配置多组阻断以及镜像口，对检测到的攻击进行旁路阻断，并可指定对端设备MAC地址。
4. 支持产品页面一键断网（禁止访问）功能，在特殊情况下，实现对特定网站的快速下线。
5. 支持防暴力破解功能，可支持频率阈值，动态令牌以及频率阈值+动态令牌等三种方式实现暴力破解防护。
6. 支持地域访问控制功能，支持根据国家、地区、城市等元素进行地域访问控制，并可自定义访问过期时长。
7. 产品具备轻量级蜜罐防御功能，提供伪造的后台管理系统页面防御功能。
8. 支持检测并清洗的攻击类型：IP攻击，TCP攻击，UDP攻击，ICMP攻击，DNS攻击，HTTP攻击等20多种DDoS攻击类型。
9. 支持入侵防护功能，并提供入侵防护特征库，特征库需要提供22种类型并提供至少14000条入侵检测特征库。
10. 支持虚拟补丁功能，支持导入appscan和RayScan扫描器的扫描结果生成WAF的规则，对此类网站漏洞直接防护。
11. 支持智能封禁，通过对网站发起的攻击次数、危害级别两个维度进行算法分析与识别，进行智能封禁，并自定义攻击者封禁时间。
12. 支持非法URL外联检测功能，针对特定外联URL进行监控或阻断，并且支持自定义URL地址。
13. 产品具备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，支持设置HTTP 0.9/1.0/1.1/2.0版本和10多种http访问控制方法。
14. 支持系统状态实时展示，需支持转发、过载、防护等三种系统状态。
15. 支持攻击态势大屏实时展示，可通过产品自带的实时态势监测模块进行攻击态势地图展示，包含对源地址、源地域、目标资产、安全防护攻击类型、攻击趋势、HTTP并发请求及实时事件的动画统计。
16. 支持日志快速响应功能，日志具备一键黑名单设置以及一键白名单排除功能。
 |
| 8 | 堡垒机系统 | 1 | 台 | 1、国产化产品，2U硬件，冗余电源；配置≥6个千兆电口，≥4个千兆光口，≥1个接口扩展槽，硬盘容量≥4T，配置国密密码卡，配置液晶屏；提供三年标准售后维保服务；2、具备≥50路图形会话或500路字符会话并发，可管理设备数量≥500个，配置500个资源授权许可；3、具备多因子认证，方式包括手机令牌、手机短信、动态令牌、国密USBKey、指纹识别等多因子认证方式；4、具备微信小程序动态口令认证方式登录堡垒机，且当用户需要使用手机令牌登录时，需要强制绑定手机令牌；5、具备对数据库协议访问操作进行控制，可基于库、表、命令实现对数据库操作的细粒度访问控制，执行动作包括但不限于断开连接、拒绝执行、动态授权、允许执行；6、不限操作系统类型，无需安装任何客户端插件，使用浏览器通过H5方式即可直接运维SSH、RDP、Telnet、VNC、Rlogin、SFTP资源；7、具备运维过程中邀请其他用户参与、协助操作；会话协同过程中，协同者可以申请控制会话，创建者可以强制获取控制权；8、具备以云盘形式在堡垒机上存储常用文件，实现操作端、堡垒机和目标资源三者之间文件共享；9、申请工单具备文件管理、RDP剪切板、磁盘映射、键盘审计、剪切板审计（上行、下行）、显示水印、上传、下载权限、OCR识别申请；10、具备采用国密算法进行重要数据加解密，包括但不限于用户信息、资源账户等；11、具备水印功能，用户在运维或者是监控、查看会话时，H5页面会将用户的登录名作为水印展示，避免数据泄露无法追责，具备在H5运维SSH、RDP、TELNET、VNC、应用发布等资源时显示水印；12、具备专属手机App远程管理（非浏览器方式），可在App端实现用户管理、主机管理、工单审批、告警消息、会话管理等功能；13、堡垒机内置文件病毒扫描能力，实现本地上传文件到堡垒机网盘、主机上传文件到堡垒机网盘的文件传输扫描，针对病毒文件，可以执行信任、删除等操作，并生成审计记录；14、产品须内置硬件国密加密卡对日志信息和访问控制信息进行完整性保护； |
| 9 | 日志审计系统 | 1 | 台 | 1. 标准1U机箱，配置≥6个10/100/1000M Base-T自适应电口，≥2个扩展槽，带1个Console口，4TB磁盘存储硬盘，冗余电源；提供三年硬件质保和软件升级服务。2. 综合日志处理性能≥4000EPS，日志采集处理均值≥11000EPS，提供210个审计节点授权许可。3. 采用B/S模式，无需安装客户端，使用WEB浏览器访问管理中心，浏览器端无需安装Java运行环境。支持chrome浏览。4. 支持通过Syslog、SNMP Trap、Netflow V5、ODBC/JDBC、Agent代理(Windows/Linux)、WMI、(S)FTP、文件共享(SMB、NetBIOS)、文件\文件夹读取、Kafka等多种方式完成各种日志的收集功能，支持多行日志采集合并为一行。5. 支持自定义资产类型及资产属性；支持对资产自定义标签，支持对标签内容进行查询和管理。6. 支持对资产IP地址的地理信息进行管理，支持单个IP、IP段设置行政区及经纬度。7. 系统提供页面可视化编辑归一化策略，对页面查看的日志编辑归一化策略，所见即所得，也支持通过归一化文件的导入来支持归一化,不需修改系统程序。8. 支持正则表达式、Key-Value、JSON日志解析，支持日志自动化辅助范化。9. 针对匹配的多条范化策略，系统支持用户手工设置策略匹配优先级。10. 日志解析字段内置130个字段，属性字段可扩展，用户可根据审计需要自行创建字段，字段类型包括IP、字符串、整型等15种，可选择映射函数等。内置及新增的所有字段均可参与查询、关联分析和报表统计。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. 支持对日志中的源和目的IP地址进行自动补全，补全IP地址的资产、国家、区域和城市等信息。13. 系统支持即席在线查询，支持嵌套查询，可针对查询结果任意回退，收敛事件范围；用户可根据需要配置事件显示的字段内容等。查询结果可支持加密导出。14. 可以以图形化的方式展示日志属性之间的聚合关系，并支持手动选择日志属性，显示多维事件分析图；属性可增加或减少，且支持图片大小调整。15. 支持将统计结果保存为仪表板、报表和策略，提供可编辑的灵活强大的自定义仪表板。16. 系统支持提供安全运维报告，帮助运维人员快速生成日常日志分析和运维报告。 |
| 10 | vpn系统 | 1 | 台 | 1. 2U设备，冗余电源，配置≧6个千兆电口，≥4个千兆SFP插槽，1个扩展槽，配置国密密码卡，4TB机械硬盘，配置250个并发用户授权，提供3年质保。
2. 支持UDP+TCP单包授权机制，UDP+TCP方式默认不开放端口，可避免业务应用的端口被扫描，进而避免利用端口对业务应用发起攻击的风险。
3. 支持通过输入安全码激活客户端，完成SPA敲门。安全码可支持共享码、一人一码两种模式。
4. 提供用户概览统计能力，包括用户总数、启用用户数、锁定用户数、禁用用户数等信息，提升管理员运维能力。
5. 支持用户身份属性的自定义扩展，以便管理员可以根据自身需要对用户属性扩展，而不需要重新部署或升级系统程序。
6. 支持用户身份打标签，以实现对不同的用户打不同标签，并可以基于标签进行细腻度访问控制。
7. 提供设备概览统计能力，包括终端总数、启用终端数、锁定终端数、禁用终端数等信息。提供设备绑定概览统计能力，包括绑定总数、管理员绑定数、申请绑定数、自助绑定数等信息，提升管理员运维能力。
8. 支持设备审批概览统计能力，管理员能够明确知道总数、待审批数、已通过数、已驳回数等信息。
9. 支持PC端发起访问应用的采集，能够对应用进行标记为可信或不可信，可用于访问控制策略，从而实现基于访问进程的细粒度控制措施。
10. 支持UOS、Kylin、Linux端操高危端口、运行的软件、零信任客户端版本、运行的杀毒软件、运行的远控软件、运行的虚拟机软件、安装的防病毒软件等环境感知和采集，以实现基于终端安全状况的访问控制措施。
11. 支持应用概览统计能力，包括应用总数、WEB应用数、隧道应用数等信息，提升管理员的运维能力。
12. 支持WEB应用支持数据传递，可通过URL、Header、Cookie自定参数传递，以满足应用对特定参数的需要，从而实现对现网应用无需修改即可正常访问。
13. 支持设备认证，提供认证策略配置，可根据是否签发设备、导入设备、绑定设备进行设备认证。
14. 支持应用限流限速功能，支持通过限制请求并发设置阈值、通过限制请求速度来设置阈值、通过限制单位时间内的请求数设置阈值、限制响应传输速率设置阈值、通过限制请求大小设置阈值。
15. 支持预防synflood攻击、忽略icmp回显请求、并支持开启ProxyProtocol来识别并传递源IP地址。
16. 支持与本项目终端安全管理系统联动，可以基于本项目终端安全管理系统对终端设备评分实现动态访问控制，提升终端安全管控能力。
 |
| 11 | 终端安全管理系统 | 1 | 套 | 1. 软件形式交付，包含控制中心和客户端软件。控制中心能够实现对客户端的集中管理，包括终端统一部署、策略配置、任务分发、集中监控、日志报表等功能；支持根据客户端点数的增加进行横向扩展；具备防病毒、补丁管理、主机防火墙、终端管控、移动存储、停服系统加固等功能，含3000个windows客户端授权；提供一年的特征库升级及维保服务。2. 客户端支持安装Windows XP\_SP3及以上/Windows Vista/Windows 7/Windows 8/Windows 10。3. 支持终端用户和管理员是一套账号管理系统，简化账号管理复杂度，一个账号解决所有身份认证，既可以用于终端登录，也可以用于管理管理中心。4. 管理控制中心当登录账号输入密码错误次数超过锁定阈值后账号将被锁定，且可设置锁定时间，该时间内账号登录请求不被接受。同时应支持双因子认证登录方式，提高安全性（投标文件需提供能够体现上述功能配置选项）。5. 客户端主程序、病毒库版本支持按分组和多批次进行灰度更新，保持在低风险中完成终端能力更新。6. 支持对进程防护、注册表防护、驱动防护、U盘安全防护、邮件防护、下载防护、IM防护、局域网文件防护、网页安全防护、勒索软件防护。7. 支持对压缩包内的病毒扫描，支持多层压缩包的扫描，可自定义配置压缩包的扫描层数，至少10层模式下的扫描。8. 支持自动阻止远程登录行为，防护黑客远程爆破和拦截恶意的远程登录。9. 支持无文件攻击防护、文档攻击防护、横移渗透攻击防护、内存攻击防护。10. 支持不少于三个杀毒引擎混合使用，提高病毒检出率。11. 支持对终端当扫描到感染型病毒、顽固木马时，自动进入深度查模式，可设置禁止终端用户管理路径或文件白名单、禁止终端用户管理扩展名白名单、扫描时不允许终端用户暂停或停止扫描任务。12. 支持扫描资源占用设置，可设置不限制、均衡型、低资源三种模式。13. 支持开启自动修复漏洞，包括开机时修复，并支持随机延迟执行、间隔修复和按时间段修复，可设置延迟时间、间隔修复时间和修复时间段。14. 支持按照补丁的维度统计补丁安装情况，包括补丁号、系统类型、补丁类型、补丁级别、补丁名称、补丁描述、发布日期、发布状态、文件数量、发现补丁次数、已安装补丁次数、忽略补丁次数、卸载补丁次数、未更新补丁库。并支持导出统计报表。15. 支持预先设置好补丁灰度发布批次漏洞修复策略，每当控制台更新补丁库，根据企业环境自动先推送给第一个小批次分组，如无问题自动推送给下一个批次，直到推送给全网。16. 支持主机防火墙功能，通过添加IP、域名规则、支持允许/拒绝规则、支持任意流向拦截和允许，支持TCP、UDP、TCP+UDP、ICMP、多播和组播，支持自定义端口范围、支持自定义目标IP，支持输入IP范围。17. 支持展示防火墙上报日志，展示终端基础信息、拦截规则名称、拦截时间、操作、协议、源地址，目的IP/域名、源端口、目的端口。18. 支持对外设进行多维度的放行，包括设备名称、PID/VID、实例路径，通过添加实现例外或加黑。19. 支持对终端节能管理，支持对长时间运行、定时关机、空闲节能、工作时间外开机等节能类型设定策略，支持仅提示、关机、注销、锁定、关闭显示器、锁定+关闭显示器、休眠和睡眠处理。并支持提示倒计时弹窗，可设置在终端取消后下一次提醒时间。20. 支持对网卡进行防护，支持阻止终端修改IP地址、使用动态IP地址、热点创建和IPV6地址使用等，可自定义提示内容和生效时间。21. 支持管理员设置自动审批客户端注册请求；不同分组可设置不同审批规则。22. 支持移动存储介质外出管理，并可以设置外出使用权限与有效时间。23. 支持U盘与终端进行点对点的授权，可以灵活控制单个U盘在不同终端上拥有不同的使用权限。24. 支持针对Windows XP、Windows7系统带来安全隐患的设计机制进行加固性修复，支持远程漏洞攻击防护、本地钓鱼攻击防护和浏览器漏洞攻击防护。 |
| 12 | 重大事件保障服务 | 1 | 项 | 在重要时期为关键信息系统提供：组织架构设计、积极防御、实时检测、响应处置、攻击预测等安全服务，以提高组织的网络安全保障能力，保障重大活动的顺利进行。 |
| 13 | 信息安全等级保护整改及相关服务 | 1 | 项 | 一、等级保护咨询 1、★执行科学的评估方法和分析体系执行科学的评估方法和分析体系，包含项目的准备及启动、信息系统识别及现状调查、明确等保评估的信息系统范围、制定等保评估工作计划、收集并分析信息系统资料、信息系统安全等级的确定、生成信息系统网络拓扑图、编写定级报告和备案信息。对信息系统的安全现状进行等级保护差距测评，分析信息系统保护现状和信息安全等级保护基本要求之间的差距，为通过信息系统等级保护奠定基础。提交《等级保护差距测评报告》。制定我单位安全需求分析、安全建设与改建方案的制定、制作原信息系统产品加固方案、测评不符合及部分符合项整改建议、制作新的网络拓扑图、制作安全需求分析报告、编制并确认整体信息系统整改方案。2、建立信息安全等级保护管理体系 根据《信息安全等级保护管理办法》和《信息系统安全等级保护基本要求》，参照《信息系统安全管理要求》、《信息系统安全工程管理要求》等标准规范要求，结合等级保护测评报告提出的安全管理体系与等级保护基本要求之间的差距，在信息安全管理制度、安全管理机构、人员安全管理、系统建设管理、系统运维管理等方面指导并协助建立健全符合相应等级要求的安全管理制度。提交《信息安全等级保护管理制度包》。3、★协助信息安全等级保护技术整改 协助我单位进行信息安全等级保护安全技术整改。根据《信息安全等级保护管理办法》和《信息系统安全等级保护基本要求》，结合等级保护测评报告提出的安全防护现状与等级保护基本要求之间的差距，综合重要信息系统的特点，明确安全需求，设计符合相应等级要求的信息系统安全技术建设整改方案，协助开展信息安全等级保护安全技术措施建设，落实相应的物理安全、网络安全、主机安全、应用安全和数据安全等安全保护技术措施。对高风险、高威胁整改完善后进行现场测评工作并出具最终报告。提交《等级保护差距整改建议》。根据项目整体目标和要求，进行安装部署调试服务，包括本次采购的设备以及业主现有的设备、主机、网络设备、安全设备和维护端设备系统，以及新增的安全设备/软件进行安全策略调整、优化，包括身份鉴别、访问控制、入侵防范、日志审计、资源管理、保密管理等进行优化。协助测评，测评公司现场实施评估和测评的时候要有安服人员在场，测评公司提出的整改需求，安服人员要及时的完成整改，保障测评全过程的顺利进行。4、★协助我单位进行三级等保测评的准备和整改工作：协助我单位进行三级等保测评的准备和整改工作。按照等级保护测评的标准，做好相关的调试整改，必须依照以下标准：《信息安全等级保护管理办法》、《信息系统安全等级保护定级指南》、《信息系统安全等级保护基本要求》、《计算机信息系统安全保护等级划分准则》（GB17859-1999）、《信息安全技术信息系统通用安全技术要求》（GB/T20271-2006）、《信息安全技术网络基础安全技术要求》（GB/T20270-2006）、《信息安全技术操作系统安全技术要求》（GB/T20272-2006）、《信息安全技术数据库管理系统安全技术要求》（GB/T20273-2006）、《信息安全技术服务器技术要求》、《信息安全技术终端计算机系统安全等级技术要求》（GA/T671-2006）等。对我单位系统安全漏洞扫描（通过专业工具）、生成信息系统漏洞扫描报告，并协助测评机构对我单位信息系统进行准备和整改。在等级保护准备和整改过程中，应采用访谈、检查、测试、工具扫描等国际国内认可的先进方法和手段进行，并与国家相关规范及标准的要求相符。必须采用专业的国内安全扫描设备及软件产品辅助整改工作的完成。对测评机构提供的第一次等保测评报告进行整改。测评机构提供的第一次等保测评报告结论为不符合的，最终要达到“基本符合”。协调信息系统优化调整（优化、调整及加固）、信息安全产品部署（上架、安装及调试）、协助建立信息系统安全管理机构、编制信息系统安全管理制度（完善）、培训信息系统安全管理人员。编写信息系统建设规划、制定信息系统运维管理制度。编写好我单位的信息系统等保所需的所有资料，包括不限于制度、流程、文件、各种记录表、登记表等所有相关文件资料。二、风险评估1、主机漏洞扫描服务 （1）内容：对被评估对象进行系统检测，利用漏洞特征，发现检查对象可能存在的主机漏洞及脆弱性;（2）支持扫描对象包括：操作系统、数据库、应用系统、网络设备、虚拟化设备1、主机操作系统扫描包括 WINDOWS、SOLARIS、AIX、LINUX、SCO、SGI等2、数据库系统扫描包括 MS-SQL、ORACLE、MYSQL、INFORMIX、SYBASE、DB2等3、应用系统扫描包括WWW、E-mail、DNS、FTP等的安全性进行漏洞扫描4、网络设备包括防火墙、路由器、交换机、IPS、IDS、堡垒机等5、★提交《漏洞扫描报告》。 |