### 包头市第四医院网络安全工具、核心系统硬件质保和网络安全运维服务采购项目服务技术要求

### 一、概述

为确保我院应用系统、网络平台、网络安全产品的稳定及安全运行，现需要采购如下软硬件产品的三年维保服务及三年期网络安全服务。

### 二、服务内容

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **名称** | **技术要求** | **数量** | **单位** | **备注** |
| 网络安全运维服务 | 详见后附 | 1 | 项 | 提供满足网络安全等级保护要求的三年服务 |
| 机房软、硬件产品维保 | 详见后附 | 1 | 项 | 提供三年维保 |

### 三、网络安全运维服务

#### 1、网络安全服务列表

|  |  |  |
| --- | --- | --- |
| **服务名称** | **详细描述** | **备注** |
| 数据库审计服务 | 服务技术要求见后附 |  |
| 系统漏扫服务 | 服务技术要求见后附 |  |
| 日志审计与分析系统服务 | 服务技术要求见后附 |  |
| 内网边界防护服务 | 服务技术要求见后附 |  |
| 外网上网行为管理服务 | 服务技术要求见后附 |  |
| 外网边界防护服务 | 服务技术要求见后附 |  |
| ▲定制安全通告 | 实时关注安全动态，为客户精心提供安全通告服务。该通告包括安全漏洞(补丁)通告、安全威胁通告、安全业界动态、恶意代码防范、紧急通告等多项内容。 | 定期开展 |
| ▲安全巡检服务 | 检查内容包括机房所有安全设备（系统）运行情况及审计日志分析、验证、重要服务器端口状况扫描、端口监听检查、用户列表检查、进程检查、病毒检查、系统木马检查等安全检查与分析工作。 | 定期开展 |
| ▲安全漏洞评估 | 使用多厂商远程漏洞评估产品，检测网络设备、操作系统、数据库和应用服务中存在的安全漏洞，提供漏洞评估报告和修复建议。 | 定期开展 |
| ▲安全配置评估 | 使用多厂商安全配置核查产品或人工方式，对系统网络设备、操作系统、数据库和应用服务器的配置进行安全检查，提供安全配置评估报告和改进建议。 | 定期开展 |
| ▲安全加固支持 | 针对安全漏洞和安全配置评估中发现的安全漏洞和配置缺陷，提供加固意见和方案，配合客户完成配置修复。 | 定期不定期结合 |
| ▲恶意样本分析 | 人工方式检测操作系统和应用中是否存在恶意样本，分析样本的访问行为，评估对系统的影响，提供安全分析报告和清除方法。 | 定期开展 |
| ▲日志安全分析 | 对各类系统产生的日志进行数据分析，及时发现攻击事件和可疑行为，提供日志分析报告。 | 定期开展 |
| ▲紧急响应 | 远程或现场方式及时响应和处理信息安全事件，协助客户降低影响，分析问题产生的原因，提供应急响应报告和改进建议。 | 不定期 |
| ▲渗透测试 | 通过人工黑盒测试方式，发现网络和业务系统中网络和系统存在的安全缺陷，提供渗透测试报告和改进建议。 | 定期开展 |
| ▲开放端口检查 | 通过扫描方式对互联网上客户开放的端口、服务进行检查，识别客户对外提供服务的真实情况。 | 定期开展 |
| ▲网站安全监测 | 通过互联网监控的方式，对客户网站进行托管式安全检测服务。当监测到用户网站遇到风险状况后，安全专家会在第一时间确认并通知用户，同时提供专业的解决方案建议。该服务内容包括远程网站漏洞扫描、网页木马监测、网页敏感内容监测、篡改监测、平稳度监测等。 | 实时监测 |
| ▲威胁检测 | 通过全网安全监测与感知预警服务（技术参数后附），发现弱点扫描、命令执行、注入攻击、跨站脚本、信息泄露、邮件钓鱼等相关风险行为。用于满足等级保护-安全区域边界中恶意代码和垃圾邮件防范的要求，以及满足安全区域边界-入侵防范中“应采取技术措施对网络行为进行分析，实现对网络攻击特别是新型网络攻击行为的分析”的高危风险要求。 | 实时监测 |
| ▲电子数据司法鉴定服务 | 对甲方重要信息系统在发生各类情况（包含但不限于故障、纠纷、投诉等等）需要开展电子数据司法鉴定的有关事宜在服务期内不限次数开展司法鉴定工作并出具具备法律效力的司法鉴定报告。 | 不定期 |

#### 2、全网安全监测与感知预警服务技术参数

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **参数性质** | **技术指标** | **技术规格要求** |
| 1 | ▲ | 服务功能模块 | 三年升级的事件库、病毒库、威胁情报库、火花H专项库 |
| 2 | ▲ | 威胁检测能力 | 需具备全面的攻击检测能力，可检测常见的Web攻击、缓冲溢出攻击、安全漏洞攻击、安全扫描攻击、拒绝服务攻击、木马后门攻击、蠕虫病毒攻击、穷举探测攻击、CGI攻击等提供功能截图； |
| 3 | ▲ | 需具备全面的Web应用类攻击检测能力，能够检测各种SQL注入攻击、XSS跨站攻击、Webshell上传、命令注入、目录遍历、命令执行等攻击行为，提供功能截图； |
| 4 |  | 提供的攻击特征不应少于6500条有效最新攻击规则，提供功能截图； |
| 5 |  | 需支持按照协议类型对攻击事件规则的设置检测有效性，协议类型包括HTTP、DNS、FTP、ICMP、IGMP、IMAP、IP、IRC、MSRPC、NETBIOS-SSN、NNTP、NTALK、PMAP、POP3、RIP、RLOGIN、SMTP、SNMP、SUNRPC、TCP、TDS、TELNET、TFTP、TNS、UDP等，提供功能截图； |
| 6 |  | 需具备攻击检测能力的扩展功能，可提供检测规则自定义的高级接口，接口具备丰富的协议变量，可以自定义配置特协议变量特征值，提供功能截图； |
| 7 |  | 需支持TCP协议攻击特征自定义，提供tcp\_ack、tcp\_fin、tcp\_flag、tcp\_payload、tcp\_syn、tcp\_urg、tcp\_seq、tcp\_rst等协议变量特征的自定义，支持设置协议变量的操作符，操作符包括等于、不等于、包含、不包含； |
| 8 |  | 需支持HTTP协议攻击特征自定义，提供http\_host、http\_method、http\_passwd、http\_url、http\_user、http\_msgbody、http\_msgbody\_len、http\_cookie、http\_user\_agent等协议变量特征的自定义，支持设置协议变量的操作符，操作符包括等于、包含或通过正则表达式设置，提供功能截图； |
| 9 |  | 需具备对事件的二次检测能力，即对已生成的事件进行二次分析与统计，并根据统计结果进行报警，支持对统计阈值进行设定的图形化用户接口，通过该图形化接口选择需要统计的基础事件并对阈值进行设置，提供功能截图； |
| 10 |  | 需具备对常见的拒绝服务攻击（DDOS）的检测能力，针对特定主机的TCP FLOOD、UDP FLOOD、ICMP FLOOD攻击行为进行检测，并支持通过控制界面配置攻击的检测时间和阈值条件，提供功能截图； |
| 11 |  | 需具Telnet、FTP、POP3、SMTP、IMAP等协议弱口令检测，并支持自定义选择弱口令检测条件，可选择的条件组合包括口令长度、口令是否包含用户名、口令是否为数字和字母组合、口令是否全为数字或者字母等，提供功能截图； |
| 12 |  | 需具备HTTP弱口令检测能力，支持配置HTTP弱口令检测用户名和密码提取关键字，不需要额外配置URL字段,检测日志中支持展示弱口令URL，提供功能截图； |
| 13 |  | 需具备攻击事件过滤能力，能够针对IP地址或MAC地址对攻击告警进行过滤，方便分析人员对正常业务造成的告警进行去除，提供功能截图； |
| 14 |  | 威胁分析能力 | 需具备提取攻击信息的能力，告警信息应包括攻击的事件名称、事件风险级别、事件安全类型、事件攻击类型、攻击者ip、受害ip、源端口、目的端口、攻击发生的时间、攻击发送次数、事件解决方案等信息，提供功能截图； |
| 15 | ▲ | 需具备事件威胁的实时事件展示能力，可以将引擎检测到的攻击在威胁展示界面进行实时显示，显示内容需全面丰富，包括：事件名称、事件风险级别、攻击ip、受害ip、事件攻击类型、事件安全类型、事件发生时间等，并支持配置实时事件展示页面自动刷新时间，方便运维展示，提供功能截图； |
| 16 |  | 需具备提取攻击行为特征信息的能力，针对产生的告警事件，可以对攻击行为特征信息进行提取并展示，方便事件分析人员对攻击行为进行分析，提供功能截图； |
| 17 | ▲ | 需具备HTTP协议攻击行为告警特征信息双向提取能力，提取内容包括攻击请求特征和完整的响应信息，方便事件分析人员对HTTP协议攻击行为进行分析，提供功能截图； |
| 18 |  | 需具备提取攻击原始报文的能力，针对产生的告警事件，可以对攻击行为的特征数据包进行提取，方便事件分析人员对攻击行为进行分析，提供功能截图； |
| 19 |  | 需支持统计近24小时木马病毒、端口扫描、拒绝服务等攻击的数量，并支持下钻查看具体攻击事件内容，支持统计近24小时攻击事件的TOP5，支持统计近24小时高危事件、中危事件、低危事件的网络威胁趋势图，提供功能截图； |
| 20 |  | 流量统计能力 | 需具备全面的流量统计能力，可以支持实时统计当前网络中的总流量、Web应用流量、数据库应用流量、邮件应用流量、P2P应用流量，并按照流量趋势图的形式进行可视化展现，提供功能截图； |
| 21 |  | 需具备强大的流量分析能力，支持根据历史流量数据，计算出当前时刻历史均值流量大小，并形成历史均值流量曲线，可以与实时流量曲线进行同时呈现并形成对比，方便分析人员掌握网络流量态势，提供功能截图； |
| 22 |  | 需具备完善的流量告警能力，支持按照历史流量同期对比和设置流量阈值两种方式配置告警参数，告警级别包含偏低、偏高等多种类型，提供功能截图； |
| 23 |  | 资产管理能力 | 需具备自动发现用户网络资产的能力，可自动上报网络中的存活资产，并支持获取内网资产的暴露面信息和资产指纹信息，提供功能截图； |
| 24 |  | 需支持自定义业务系统资产分组的能力，可将发现的资产自动划分至所属的业务系统资产分组，业务系统资产分组应至少支持五级，提供功能截图； |
| 25 |  | 需具备未知（非法）资产入网发现的能力，可以及时发现违规入网的IP地址，防止内网资产乱接乱用，提供功能截图； |
| 26 |  | 流数据采集与互联分析能力 | 需具备将网络流量数据解析成资产设备间互联访问关系的能力，能够详细记录源IP、源IP分组、源IP地区、目的IP、目的IP分组、目的IP地区、目的端口、传输层协议、服务名称、流量大小、频次等数据信息，提供功能截图； |
| 27 |  | 需具备自动发现内部资产与互联网设备互联的能力，并能准确显示互联的方向，能够区分是内部服务器向外发起连接还是外部设备向用户内部服务器发起的连接，提供功能截图； |
| 28 | ▲ | 需具备将网络流量按照业务系统资产分组可视化展示互联关系的能力，支持拓扑图的形式展示内网和互联网以及内网各域之间互联情况，方便分析人员全面掌握全网访问关系，提供功能截图； |
| 29 | ▲ | 需具备可视化展示各业务系统资产分组互联关系的能力，支持查看资产分组内的互联情况和资产分组之间的互联情况，方便分析人员分析，提供功能截图； |
| 30 |  | 需具备监控违规访问互联网和非法连接的能力，支持对网络中产生的违规互联进行实时告警，并用红色连线在互联拓扑图中进行标识，方便分析人员快速发现违规外联和非法访问，提供功能截图； |
| 31 |  | 支持内置网络主机异常行为特征算法（非数据包特征），通过主机的互联行为可以主动发现内网具有一定威胁的异常主机，包括中招蠕虫主机、网络扫描主机等，提供功能截图； |
| 32 |  | 需具备应用层协议解析能力，支持解析HTTP协议URL数据、DNS协议域名数据等应用层数据信息，提供功能截图； |
| 33 | ▲ | 系统管理能力 | 需具备检测策略管理能力，支持检测策略规则可以按照协议类型、攻击类型、安全类型、影响系统、影响设备等多个维度进行展示，方便运维人员按照不同的业务场景创建检测策略集，提供功能截图； |
| 34 |  | 需具备邮件告警能力，支持将发现的攻击告警信息通过邮件的方式发送至指定的邮箱地址，提供功能截图； |
| 35 |  | 需具备完善的特征库升级能力，特征库升级支持在线和离线升级方式，通过关官网下载离线升级特征库后，支持web界面一键导入方式进行升级； |
| 36 |  | 需具备探针设备的监控能力，实时监控检测引擎的连接状态、当前使用的检测策略集和设备的资源配置信息，提供功能截图； |
| 37 |  | 需支持多级部署、集中管理能力，可以添加组件（包括控制中心、引擎），至少支持五级以上部署环境； |
| 38 |  | 级联环境中，系统需具备支持上级对下级转发事件库升级包、系统升级补丁包，上级控制中心可以对下级统一下发策略集，方便统一管理； |
| 39 |  | 需具备Web界面服务配置能力，可配置启用/停用http和https服务，支持配置http和https访问设备WEB界面端口，提供功能截图； |
| 40 |  | 需具备Web页面登录命令行进行系统配置，提供功能截图； |
| 41 |  | 需具备用户管理能力，支持三权分立原则，系统具有用户管理员、审计管理员、配置管理员，支持创建不同的配置管理员，并赋予不同的授权角色，控制管理员的配置权限，提供功能截图； |
| 42 |  | 需具备绑定管理员用户IP地址的能力，支持对管理员用户的IP地址进行绑定，防止非法IP的使用账号访问设备，提供功能截图； |
| 43 |  | 需具备WEB页面对数据库进行初始化，初始化后设备检测日志记录清空，且不影响设备正常功能使用，提供功能截图； |
| 44 |  | 报表分析能力 | 需具备多种数据报表类型，每种报表类型的数据统计方式应从不同的维度进行分析，方便不同层次的技术人员进行数据汇总，提供功能截图； |
| 45 |  | 需具备数据交叉统计能力，支持按照事件名称、源地址、目的地址等多个维度对事件进行交叉统计分析，帮助分析人员快速定位攻击，提供功能截图； |
| 46 |  | 报表需支持如下格式：HTML、PDF、EXCEL、WORD、WPS、PFD、UOF，所生成的报表可以自动发送到多个邮箱，能辅助用户查阅，提供功能截图； |
| 47 |  | 报表需支持手动立即执行、周期性自动执行两种执行方式，提供功能截图； |

#### 3、数据库审计服务

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **参数性质** | **技术指标** | **技术规格要求** |
|  | ▲ | 基础服务内容 | 审计存储容量不小于4T，可审计数据库不少于16个，含不少于8个虚拟化中的数据库审计。 |
|  | ▲ | 性能要求 | SQL峰值处理能力：≥20000条/秒，在线日志总量：≥100亿条 |
|  |  | 服务方式 | 支持在目标数据库服务器主机上安装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（不需要提供DBA账号和任何数据库账户，不需要创建任何数据库账户），审计平台可以实时监控agent CPU使用率、内存使用率、传输包个数。 |
|  |  | agent参数支持自定义，支持IP(IPv4\IPv6)、CPU占用率、内存占用率、本地缓存大小、端口等灵活配置。 |
|  |  | 支持审计平台WEB界面管理插件，支持插件的配置、唤醒、挂起、中断、升级，审计平台支持远程安装、卸载、下载。 |
|  |  | 协议支持 | Oracle、SQL Server、MySQL、MariaDB、AnalyticDB、DB2、达梦DM、Informix、Domino、PostgreSQL、Sybase、GBase、Cache、KingBase、OSCAR、MongoDB、HANA、OceanBase、PolarDB等等。 |
|  |  | 支持同时对传统数据库和大数据数据库进行审计。 |
|  |  | 支持对数据库协议的编码进行自识别。 |
|  |  | 审计功能智能发现服务 | 支持基于深度协议解析技术自动发现数据库，并完成自动添加和审计。不主动扫描，避免对数据库性能造成影响。 |
|  |  | 应用关联服务 | 支持4层应用关联，能够识别应用用户及URL。 |
|  |  | 安全审计服务 | 满足三权分立，审计用户仅审计系统管理员、安全管理员操作行为，安全管理员审计“审计管理员”操作行为。 |
|  |  | 审计策略服务 | 内置安全事件维度策略组，同时支持自定义添加。 |
|  |  | 内置数据库类型维度策略组，同时支持自定义添加。 |
|  |  | 内置SQL注入维度策略组，同时支持自定义添加。 |
|  |  | 内置高危行为维度策略组，同时支持自定义添加。 |
|  |  | 审计服务 | 支持记录SQL语句执行时间、业务用户名、操作终端主机名及IP地址、终端工具名称、服务器端主机名及IP地址、数据库名、表名、SQL语句、响应时间、返回结果等关键信息。 |
|  |  | 支持对SQL语句执行结果（成功/失败）、SQL语句执行时间、SQL语句执行异常等数据库操作响应信息的审计。 |
|  |  | 支持对于符合条件的SQL语句过滤，避免脏数据冗余。 |
|  | ▲ | 支持审计和告警语句会话回放。提供截图证明文件。 |
|  |  | 支持更精简的SQL摘要元素。 |
|  | ▲ | 审计日志导出控制，需要输入密码认证。提供截图证明文件。 |
|  |  | 对数据库客户端工具运行过程中自动产生的SQL语句的过滤，减少不必要的审计记录。 |
|  |  | 统计分析服务 | 支持从多维度对数据资产、日志数量、风险数量、SQL流量进行展示。 |
|  |  | 支持按SQL操作类型、事件类型、风险级别、来源、SQL流量等多维度进行统计分析。 |
|  |  | 支持对统计数据进行下钻分析、以图表方式展示分析结果。 |
|  |  | 统计报表服务 | 系统内置PCI、SOX、等级保护等多种行业报表模板。 |
|  |  | 系统内置数据库流量统计、告警IP、SQL摘要、用户操作明细等统计报表。 |
|  |  | 系统支持完全自定义报表，用户可自定义报表内容、报表条件。 |
|  |  | 支持告警信息重新发送、告警信息发送情况统计等。 |
|  |  | 报表输出格式支持：PDF、EXCEL、WORD。 |

#### 4、系统漏扫服务

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **参数性质** | **技术指标** | **技术规格要求** |
|  | ▲ | 服务内容 | 支持常规漏扫服务外，还支持WEB漏扫、配置核查功能，支持无限IP。 |

#### 5、日志审计与分析系统服务

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **参数性质** | **技术指标** | **技术规格要求** |
|  | ▲ | 基础服务内容 | 日志存储容量≥2TB，≥300个被审计服务对象。 |
|  | ▲ | 性能指标 | 日志处理性能≥2000EPS。 |
|  |  | 日志采集 | 支持SNMP Trap、Syslog、ODBC\JDBC、文件\文件夹、WMI、FTP、SFTP、NetBIOS、OPSEC等多种方式完成日志收集功能. |
|  |  | 资产管理服务 | 资产模块支持对资产的ping、telnet和远程访问等功能；需提供功能截图 |
|  | ▲ | 系统提供基于资产的拓扑视图，可以按列表和拓扑两种模式显示资产拓扑节点；可查看每个资产设备本身产生的事件信息、关联告警信息，并且支持向下钻取，直接进入事件列表、关联告警列表；需提供功能截图 |
|  |  | 能够根据收到事件的设备地址自动识别新的资产并自动添加到资产库中。需提供功能截图 |
|  |  | 工作台展示 | 系统必须内置基本的仪表板。用户可以在工作台中自定义仪表板，按需设计仪表板显示的内容和布局，可以为用户建立不同维度的仪表板；需提供功能截图 |
|  |  | 仪表板中的每个显示区域都能够放大、缩小、拖动；需提供功能截图。 |
|  |  | 日志管理服务 | 对不支持的事件类型提供可扩展功能；支持长安全事件格式；对日志设备类型、日志类型、日志级别等可进行重定义； |
|  |  | 日志可加密压缩传输 支持加密压缩方式转发，定时转发；需提供功能截图 |
|  |  | 支持对日志的过滤和合并；合并支持设定合并的时间范围； |
|  |  | 支持日志源管理功能，对断点日志源可以设置产生告警，单个日志源设备查看该设备最近7天的事件趋势。需提供功能截图 |
|  |  | 并提供基于日志查询任务模式的日志导出功能。需提供功能截图 |
|  | ▲ | 日志范式化服务 | 范式化字段至少应包括事件接收时间、事件产生时间、事件持续时间、用户名称、源地址、源MAC地址、源端口、操作、目的地址、目的MAC地址、目的端口、事件名称、事件摘要、等级、原始等级、原始类型、网络协议、网络应用协议、设备地址、设备名称、设备类型等；针对不支持的事件类型做范式化不需改动编码，通过修改配置文件即可完成。需提供功能截图 |
|  | ▲ | 产品界面支持范式化文件的导入导出功能。需提供功能截图 |
|  | ▲ | 日志分析服务 | 系统需内置不同分析场景，包括各种实时分析场景、历史统计场景、实时统计等。并支持支持自定义场景； |
|  | ▲ | 可以手工对选中的日志进行一键告警或者加入观察列表中；需提供功能截图 |
|  | ▲ | 自定义事件查询策略，基于事件分类的查询条件不少于10大项50小项。需提供功能截图 |
|  | ▲ | 可以对选中的日志提供在线/离线地图定位、源IP与目的IP分布走向的视网膜图展示、描述日志之间行为相关关系的事件拓扑图等多种分析工具；需提供功能截图 |
|  |  | 统计分析模式下支持柱状图、饼图等形式的统计信息可视化展示；根据统计结果可直接钻取符合条件的日志。 |
|  | ▲ | 关联分析服务 | 提供基于图形化方式的规则编辑器；规则支持新增、删除、移动、复制、导入和导出等动作；需提供功能截图 |
|  |  | 所有事件字段都可参与关联，规则可实时启用和停用。 |
|  | ▲ | 在编辑规则条件的时候，可以针对事件属性引用规则、应用资产属性、引用资源需提供功能截图； |
|  |  | 可实现统计计数关联，能够设定一段时间内的事件发生次数的阈值，还能指定重复事件的属性特征进行事件合并需提供功能截图； |
|  | ▲ | 资源服务 | 可以将日志中的IP地址、端口、时间等信息进行资源自定义，为规则所引用需提供功能截图 |
|  |  | 告警响应服务 | 告警动作支持告警重定义、弹出提示框、发出警示音、发送邮件、发送SNMP Trap、发送短信、执行命令脚本、设备联动、发送飞鸽传书、发送Syslog、加入观察列表、从观察列表中删除；需提供功能截图 |
|  |  | 具备告警抑制功能，可以把同一时间内相同的告警合并成一条事件进行展示。告警抑制规则中的时间范围与合并数目可以手动进行配置；告警抑制规则可实时启用和停用。 |
|  |  | 综合显示服务 | 能够显示告警状态雷达图，日志趋势曲线图；最近事件览图；最近一段时间不同日志分类的日志数量，不同等级的日志的数量，事件EPS曲线。需提供功能截图 |

#### 6、内网边界防护服务

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **参数性质** | **技术指标** | **技术规格要求** |
|  | ▲ | 基础服务内容 | 三年服务的IPS特征库、防病毒特征库、WEB应用防护库、威胁情报库、应用识别及URL分类库。 |
|  | ▲ | 性能要求 | 同时开启边界防护+APP+AV+IPS时网络吞吐≥20G，同时开启边界防护+APP识别+IPS+AV时应用层吞吐≥12G，同时开启边界防护+APP识别+IPS+AV时最大并发连接数≥280万。 |
|  |  | 基础网络支持服务 | 支持静态路由、RIP、RIPng、OSPFv2、OSPFv3、BGP、ISP路由； |
|  |  | 内置移动、联通、电信、教育网、网通、长城宽带等ISP服务商地址列表； |
|  | ▲ | 内置世界各国ISP地址库；需提供功能截图。 |
|  |  | 支持802.1q，支持stp； |
|  | ▲ | 支持根据入接口、源/目的IP地址、源/目的端口、协议、用户、应用、选路算法、探测、度量值、权重等多种条件设置策略路由；  支持不少于8种的选路算法；需提供功能截图。 |
|  | ▲ | 支持手动和LACP链路聚合，可根据源/目的mac、目的IP、等条件提供不少于2种链路负载算法；需提供功能截图。 |
|  | ▲ | 支持IPv4/v6双栈；需提供功能截图。； |
|  |  | IP/MAC静态和动态探测绑定； |
|  |  | 支持源NAT、目的NAT、静态NAT，支持一对一、一对多和多对多等形式的NAT；支持Sticky NAT开关，使相同源IP的数据包经过地址转换后为其转换的源 IP 地址相同；需提供功能截图。 |
|  |  | 支持NAT64, NAT46支持静态转换和前缀转换方式；需提供功能截图。 |
|  |  | 支持 NAT66地址转换，支持源地址转换，目的地址转换，静态地址转换； |
|  |  | 支持NAT源端口复用，单个公网IP支持的并发会话数量无限制； |
|  |  | 支持SNAT源端口保持功能； |
|  |  | 支持NAT策略冲突检测； |
|  |  | 支持NAT地址池利用率告警； |
|  | ▲ | 支持DNS Doctoring功能，能够将来自内部网络的域名解析请求定向到真实内网资源，提高访问效率，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；需提供功能截图。 |
|  |  | 支持各种应用协议的NAT穿越：FTP、TFTP、H.323、SQL＊NET； |
|  |  | 支持标准DHCP服务功能，支持DHCP条件下的IP/MAC绑定及IP地址排除等功能； |
|  |  | 支持DNS透明代理功能，可将指定范围内的DNS请求自动重定向至管理员指定的DNS服务器，且支持多台DNS服务器的负载均衡；需提供功能截图。 |
|  |  | 支持标准DNS服务器功能，支持多种DNS 记录 ，包括A ，NS，CNMAE，TXT，MX，PTR记录；需提供功能截图。 |
|  | ▲ | 访问控制服务 | 支持Web认证，在策略中可设置用户 Web 认证的门户地址；需提供功能截图。 |
|  | ▲ | 支持基于策略的流量统计和会话统计； |
|  | ▲ | 提供策略分析功能，支持策略命中分析、策略冗余分析、策略冲突检查、策略包含分析，可在WEB界面显示检测结果；需提供功能截图。 |
|  |  | 支持策略加速技术，减少策略对设备性能的消耗；需提供功能截图。 |
|  | ▲ | 支持详细的访问控制策略日志，每条匹配策略的会话均可记录其建立会话和拆除会话的日志；访问控制策略日志可本地记录或发送至Syslog服务器；需提供功能截图。 |
|  |  | 提供策略查询功能，支持五元组快速查询以及针对策略名、源/目的区域、源/目的地址、服务、对象、策略命中数等条件进行细粒度查询；需提供功能截图。 |
|  | ▲ | 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；需提供功能截图。 |
|  | ▲ | IPv6安全防护服务 | 支持基于IPv6的入侵防御、病毒防御、DDOS、WEB防护、防御等一系列安全防护功能；需提供功能截图。 |
|  | ▲ | 支持基于IPv6的流量控制、连接限制；需提供功能截图。 |
|  | ▲ | 入侵防御服务 | 支持独立的入侵防护规则特征库，特征总数在7000条以上，能对常见漏洞进行安全防护；需提供功能截图。 |
|  | ▲ | 规则库支持根据攻击类型、风险等级、流行程度等进行分类，防护动作包括告警、阻断；需提供功能截图。 |
|  |  | 支持针对地址设置入侵防御白名单，支持攻击规则搜索以及自定义；需提供功能截图。 |
|  |  | DDOS防御服务 | 支持针对ICMP、TCP、UDP、等协议进行DDOS防护；支持预定义和自定义策略模板； |
|  |  | 病毒过滤服务 | 支持对HTTP/SMTP/POP3/FTP/IMAP等协议进行病毒防御；需提供功能截图。 |
|  | ▲ | 病毒特征库规模超过1200万；需提供功能截图。 |
|  |  | Web防护服务 | 支持对100个站点制订web应用防护策略，支持http请求回应的头、体检查； |
|  |  | 支持自定义web安全防护事件，可以对请求参数、各个头域、内容关键字、文件类型等进行灵活组合生成策略；需提供功能截图。 |
|  | ▲ | 支持对http的合规性检查，包括版本、方法、url、头域字段、传输文件等的合规性检查；需提供功能截图。 |
|  |  | 内置web应用防护特征库，提供定期升级 |
|  |  | 弱口令检查服务 | 支持对HTTP、telnet、FTP、SMTP、POP3等各种协议进行弱口令检查，并上报安全事件；需提供功能截图。 |
|  |  | 支持高、中、低三种密码检查强度； |
|  |  | 支持对源目的ip地址进行过滤检查； |
|  |  | 过滤服务 | 可设置基于IP过滤条件，实现对特定报文进行快速过滤，支持100万以上黑名单数量；需提供功能截图。 |
|  | ▲ | 内置动态黑名单功能，可与URL过滤、病毒过滤功能实现联动封锁；支持静态和动态黑名单命中统计和监控；支持黑名单添加事件和生效时间展示；需提供功能截图。 |
|  | ▲ | 支持黑名单多种类型导入，如通过文件上传增量添加黑名单、支持页面复制粘贴方式添加黑名单、支持API接口下发黑名单；需提供功能截图。 |
|  |  | 支持按照ip/ip网段模糊检索； |
|  |  | 黑名单列表支持展示添加时间、添加方式（手工或来自其他安全事件）、命中次数。并支持按照命中次数排序； |
|  | ▲ | 应用控制/URL过滤服务 | 支持IPv6的应用控制策略； |
|  |  | 支持并开通基于DPI和DFI技术的应用特征识别及行为控制，应用识别的种类不少于2000种； |
|  |  | 支持针对应用动作、应用内容的细粒度控制，如设定允许登录的QQ帐号白名单、邮件关键字过滤等； |
|  |  | 支持并开通WEB控制功能模块，包括URL访问分类管理、网页关键字过滤、http文件下载类型管理等功能；需提供功能截图。 |
|  |  | URL分类库规模不少于2000万条；需提供功能截图。 |
|  |  | 内置P2P应用、网页应用、数据库应用等应用特征库；需提供功能截图。 |
|  | ▲ | 支持超过100类、2000万的URL地址分类库，用户可根据网站类别对自身网络的WEB应用实施全面化管控，杜绝非法、违规网站的访问行为； |
|  | ▲ | 带宽管理服务 | 支持链路和四层通道嵌套的流量控制功能，可基于上下行区域、地址、地理对象、用户/用户组、服务/服务组、应用/应用组和时间等配置带宽策略，支持带宽策略优先级；需提供功能截图。 |
|  |  | 支持带宽限制、带宽保障和弹性带宽； |
|  |  | 支持高、中、低优先级通道设置； |
|  | ▲ | 连接控制服务 | 支持对指定的源/目的地址对象、源/目的地理对象、应用制定连接限制策略，可控制所有或单IP会话总数及单IP新建连接数；需提供功能截图。 |
|  | ▲ | 用户管控服务 | 内置强大的用户身份管理系统，支持本地认证、外部认证及等方式，支持RADIUS、LDAP等第三方外部认证； |
|  | ▲ | 支持防暴力破解、密码复杂度、密码有效性设置，如认证失败次数及锁定时间、密码格式、密码长度、首次登陆修改密码、密码定期修改、密码有效时间等设置； |
|  | ▲ | 支持查看在线用户情况和用户流量，可显示用户流量、会话、新建连接列表及趋势图，支持用户流量排名；需提供功能截图。 |
|  | ▲ | 支持本地CA和第三方CA，支持作为CA认证中心为其他人签发证书，也可采用第三方CA为其他人签发证书，支持标准CRL列表，支持CRL手工更新；需提供功能截图。 |
|  |  | IPSEC VPN服务 | 支持IPSec VPN功能，支持IKEV1、IKEV2、国密的加密类型，支持AES、DES、3DES、MD5、SHA-1、SM3等VPN加密、认证算法，支持对隧道内网络流量进行监控展示；需提供功能截图。 |
|  | ▲ | 无需额外授权，IPSec VPN用户数无限制； |
|  |  | 支持硬件国密加速卡(部分型号支持)； |
|  | ▲ | SSL VPN服务 | 支持SSL VPN功能，满足远程用户安全接入内网； |
|  | ▲ | 无需额外授权，SSL VPN用户数无限制； |
|  |  | SSL VPN支持代理模式，能够直接代理内网页面到VPN用户登录页面； |
|  |  | SSL VPN支持隧道模式，可添加多条路由，满足多网段内网的访问需求； |
|  |  | SSL vpn支持BBR加速，在高延时、丢包等不良网络条件下，可以提升传输效率3-5倍以上 |
|  |  | SSL VPN登录支持双因子认证； |
|  | ▲ | 防护结果监控服务 | 支持对状态、威胁信息、接口流量、连接信息、应用流量、用户流量、网站类型流量、VPN流量、在线用户等对象进行监控展示；需提供功能截图。 |
|  |  | 支持对CPU、内存、整机流量、新建、并发进行统计，展示CPU、内存实时利用率及其历史走势图； |
|  |  | 支持威胁可视化技术和流量可视化技术，可提供详细的分析展示图表；需提供功能截图。 |
|  |  | 支持主机威胁统计和展示，包括基于地理位置的威胁地图展示、基于威胁级别和威胁类型的统计分析、基于威胁事件源/目的主机的TOP10统计展示、基于具体威胁事件/威胁类型的TOP10统计展示等，统计展示的时间周期包括1小时/1天/7天/30天；需提供功能截图。 |
|  |  | 支持根据应用对通过的数据进行统计，包括应用总流量排名和各个应用的协议名称、总流量、上行流量、下行流量、流速； |
|  |  | 支持基于流量的TOP100用户和TOP100应用的流量曲线图，流量曲线图的统计周期包括小时、天、7天和30天；需提供功能截图。 |
|  |  | 系统统计详情。针对总流量、CPU、内存利用率，并发连接，新建连接，做72小时精细化曲线统计，曲线支持局部放大。 |
|  | ▲ | 日志服务 | 支持标准syslog协议 |
|  |  | 支持日志合并功能，相同类型的日志支持合并操作，降低日志流量开销；需提供功能截图。 |
|  |  | 支持日志外发至多个SYSLOG服务器； |
|  |  | 支持流日志功能，将每一条数据流生命周期的各个业务模块的操作，整合为一条完整的日志进行展示；需提供功能截图。 |
|  | ▲ | 威胁情报防护服务 | 支持基于威胁情报云的动态防护功能，支持将用户对互联网的访问信息发送至威胁情报云进行实时情报查询及防护。提供配置界面及威胁情报云端界面截图； |
|  | ▲ | 威胁情报具备云端汇集实时热点高威胁情报数据，提供边界防御研判恶意可疑行为，区分高频随机性攻击与高危定向攻击，预判并阻断攻击威胁对业务的影响； |
|  | ▲ | 威胁情报类型包括可疑行为（垃圾邮件、网络爬虫、挖矿、主机扫描）、攻击威胁（网银大盗、爆破攻击、DDoS攻击、漏洞利用、Web漏洞攻击）、恶意站点（欺诈、赌博、钓鱼）、恶意软件（黑客工具、宏病毒、勒索软件、远控木马、网络蠕虫）、攻击组织（APT组织、僵尸网络C2、IoT攻击C2）、失陷主机（僵尸主机、IoT失陷主机）等； |
|  |  | 策略梳理服务 | 支持扩展集中策略分析模块；需提供功能截图。 |
|  |  | 支持集中对所有安全策略进行冗余分析，可分析出安全策略是否为不必要的冗余配置；需提供功能截图。 |
|  |  | 支持集中对所有安全策略进行收敛分析，也称宽松策略分析。能够支持查看任何一条宽松策略的流量详细信息；需提供功能截图。 |
|  |  | 支持集中对所有安全策略进行命中频率分析，辅助用户快速完成策略次序的调整，从而达到优化边界防护处理性能的目的；需提供功能截图。 |
|  |  | 支持集中对所有安全策略进行潜在冲突分析，辅助用户快速完成策略的调整，从而达到访问控制的目的；需提供功能截图。 |

#### 7、外网上网行为管理服务

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **参数性质** | **技术指标** | **技术规格要求** |
|  | ▲ | 服务内容 | 上网行为管理服务支持的网络层吞吐量（大包）：≥3.6Gb，支持三年的URL&应用识别规则库服务。 |

#### 8、外网边界防护服务

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **参数性质** | **技术指标** | **技术规格要求** |
|  | ▲ | 基础服务内容 | 三年服务的IPS特征库、防病毒特征库、WEB应用防护库、威胁情报库、应用识别及URL分类库。 |
|  | ▲ | 性能要求 | 同时开启边界防护+APP+AV+IPS时网络吞吐≥8G。 |
|  |  | 基础网络支持服务 | 支持静态路由、RIP、RIPng、OSPFv2、OSPFv3、BGP、ISP路由； |
|  |  | 内置移动、联通、电信、教育网、网通、长城宽带等ISP服务商地址列表； |
|  | ▲ | 内置世界各国ISP地址库；需提供功能截图。 |
|  |  | 支持802.1q，支持stp； |
|  | ▲ | 支持根据入接口、源/目的IP地址、源/目的端口、协议、用户、应用、选路算法、探测、度量值、权重等多种条件设置策略路由；  支持不少于8种的选路算法；需提供功能截图。 |
|  | ▲ | 支持手动和LACP链路聚合，可根据源/目的mac、目的IP、等条件提供不少于2种链路负载算法；需提供功能截图。 |
|  | ▲ | 支持IPv4/v6双栈；需提供功能截图。； |
|  |  | IP/MAC静态和动态探测绑定； |
|  |  | 支持源NAT、目的NAT、静态NAT，支持一对一、一对多和多对多等形式的NAT；支持Sticky NAT开关，使相同源IP的数据包经过地址转换后为其转换的源 IP 地址相同；需提供功能截图。 |
|  |  | 支持NAT64, NAT46支持静态转换和前缀转换方式；需提供功能截图。 |
|  |  | 支持 NAT66地址转换，支持源地址转换，目的地址转换，静态地址转换； |
|  |  | 支持NAT源端口复用，单个公网IP支持的并发会话数量无限制； |
|  |  | 支持SNAT源端口保持功能； |
|  |  | 支持NAT策略冲突检测； |
|  |  | 支持NAT地址池利用率告警； |
|  | ▲ | 支持DNS Doctoring功能，能够将来自内部网络的域名解析请求定向到真实内网资源，提高访问效率，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；需提供功能截图。 |
|  |  | 支持各种应用协议的NAT穿越：FTP、TFTP、H.323、SQL＊NET； |
|  |  | 支持标准DHCP服务功能，支持DHCP条件下的IP/MAC绑定及IP地址排除等功能； |
|  |  | 支持DNS透明代理功能，可将指定范围内的DNS请求自动重定向至管理员指定的DNS服务器，且支持多台DNS服务器的负载均衡；需提供功能截图。 |
|  |  | 支持标准DNS服务器功能，支持多种DNS 记录 ，包括A ，NS，CNMAE，TXT，MX，PTR记录；需提供功能截图。 |
|  | ▲ | 访问控制服务 | 支持Web认证，在策略中可设置用户 Web 认证的门户地址；需提供功能截图。 |
|  | ▲ | 支持基于策略的流量统计和会话统计； |
|  | ▲ | 提供策略分析功能，支持策略命中分析、策略冗余分析、策略冲突检查、策略包含分析，可在WEB界面显示检测结果；需提供功能截图。 |
|  |  | 支持策略加速技术，减少策略对设备性能的消耗；需提供功能截图。 |
|  | ▲ | 支持详细的访问控制策略日志，每条匹配策略的会话均可记录其建立会话和拆除会话的日志；访问控制策略日志可本地记录或发送至Syslog服务器；需提供功能截图。 |
|  |  | 提供策略查询功能，支持五元组快速查询以及针对策略名、源/目的区域、源/目的地址、服务、对象、策略命中数等条件进行细粒度查询；需提供功能截图。 |
|  | ▲ | 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；需提供功能截图。 |
|  | ▲ | IPv6安全防护服务 | 支持基于IPv6的入侵防御、病毒防御、DDOS、WEB防护、防御等一系列安全防护功能；需提供功能截图。 |
|  | ▲ | 支持基于IPv6的流量控制、连接限制；需提供功能截图。 |
|  | ▲ | 入侵防御服务 | 支持独立的入侵防护规则特征库，特征总数在7000条以上，能对常见漏洞进行安全防护；需提供功能截图。 |
|  | ▲ | 规则库支持根据攻击类型、风险等级、流行程度等进行分类，防护动作包括告警、阻断；需提供功能截图。 |
|  |  | 支持针对地址设置入侵防御白名单，支持攻击规则搜索以及自定义；需提供功能截图。 |
|  |  | DDOS防御服务 | 支持针对ICMP、TCP、UDP、等协议进行DDOS防护；支持预定义和自定义策略模板； |
|  |  | 病毒过滤服务 | 支持对HTTP/SMTP/POP3/FTP/IMAP等协议进行病毒防御；需提供功能截图。 |
|  | ▲ | 病毒特征库规模超过1200万；需提供功能截图。 |
|  |  | Web防护服务 | 支持对100个站点制订web应用防护策略，支持http请求回应的头、体检查； |
|  |  | 支持自定义web安全防护事件，可以对请求参数、各个头域、内容关键字、文件类型等进行灵活组合生成策略；需提供功能截图。 |
|  | ▲ | 支持对http的合规性检查，包括版本、方法、url、头域字段、传输文件等的合规性检查；需提供功能截图。 |
|  |  | 内置web应用防护特征库，提供定期升级 |
|  |  | 弱口令检查服务 | 支持对HTTP、telnet、FTP、SMTP、POP3等各种协议进行弱口令检查，并上报安全事件；需提供功能截图。 |
|  |  | 支持高、中、低三种密码检查强度； |
|  |  | 支持对源目的ip地址进行过滤检查； |
|  |  | 过滤服务 | 可设置基于IP过滤条件，实现对特定报文进行快速过滤，支持100万以上黑名单数量；需提供功能截图。 |
|  | ▲ | 内置动态黑名单功能，可与URL过滤、病毒过滤功能实现联动封锁；支持静态和动态黑名单命中统计和监控；支持黑名单添加事件和生效时间展示；需提供功能截图。 |
|  | ▲ | 支持黑名单多种类型导入，如通过文件上传增量添加黑名单、支持页面复制粘贴方式添加黑名单、支持API接口下发黑名单；需提供功能截图。 |
|  |  | 支持按照ip/ip网段模糊检索； |
|  |  | 黑名单列表支持展示添加时间、添加方式（手工或来自其他安全事件）、命中次数。并支持按照命中次数排序； |
|  | ▲ | 应用控制/URL过滤服务 | 支持IPv6的应用控制策略； |
|  |  | 支持并开通基于DPI和DFI技术的应用特征识别及行为控制，应用识别的种类不少于2000种； |
|  |  | 支持针对应用动作、应用内容的细粒度控制，如设定允许登录的QQ帐号白名单、邮件关键字过滤等； |
|  |  | 支持并开通WEB控制功能模块，包括URL访问分类管理、网页关键字过滤、http文件下载类型管理等功能；需提供功能截图。 |
|  |  | URL分类库规模不少于2000万条；需提供功能截图。 |
|  |  | 内置P2P应用、网页应用、数据库应用等应用特征库；需提供功能截图。 |
|  | ▲ | 支持超过100类、2000万的URL地址分类库，用户可根据网站类别对自身网络的WEB应用实施全面化管控，杜绝非法、违规网站的访问行为； |
|  | ▲ | 带宽管理服务 | 支持链路和四层通道嵌套的流量控制功能，可基于上下行区域、地址、地理对象、用户/用户组、服务/服务组、应用/应用组和时间等配置带宽策略，支持带宽策略优先级；需提供功能截图。 |
|  |  | 支持带宽限制、带宽保障和弹性带宽； |
|  |  | 支持高、中、低优先级通道设置； |
|  | ▲ | 连接控制服务 | 支持对指定的源/目的地址对象、源/目的地理对象、应用制定连接限制策略，可控制所有或单IP会话总数及单IP新建连接数；需提供功能截图。 |
|  | ▲ | 用户管控服务 | 内置强大的用户身份管理系统，支持本地认证、外部认证及等方式，支持RADIUS、LDAP等第三方外部认证； |
|  | ▲ | 支持防暴力破解、密码复杂度、密码有效性设置，如认证失败次数及锁定时间、密码格式、密码长度、首次登陆修改密码、密码定期修改、密码有效时间等设置； |
|  | ▲ | 支持查看在线用户情况和用户流量，可显示用户流量、会话、新建连接列表及趋势图，支持用户流量排名；需提供功能截图。 |
|  | ▲ | 支持本地CA和第三方CA，支持作为CA认证中心为其他人签发证书，也可采用第三方CA为其他人签发证书，支持标准CRL列表，支持CRL手工更新；需提供功能截图。 |
|  |  | IPSEC VPN服务 | 支持IPSec VPN功能，支持IKEV1、IKEV2、国密的加密类型，支持AES、DES、3DES、MD5、SHA-1、SM3等VPN加密、认证算法，支持对隧道内网络流量进行监控展示；需提供功能截图。 |
|  | ▲ | 无需额外授权，IPSec VPN用户数无限制； |
|  |  | 支持硬件国密加速卡(部分型号支持)； |
|  | ▲ | SSL VPN服务 | 支持SSL VPN功能，满足远程用户安全接入内网； |
|  | ▲ | 无需额外授权，SSL VPN用户数无限制； |
|  |  | SSL VPN支持代理模式，能够直接代理内网页面到VPN用户登录页面； |
|  |  | SSL VPN支持隧道模式，可添加多条路由，满足多网段内网的访问需求； |
|  |  | SSL vpn支持BBR加速，在高延时、丢包等不良网络条件下，可以提升传输效率3-5倍以上 |
|  |  | SSL VPN登录支持双因子认证； |
|  | ▲ | 防护结果监控服务 | 支持对状态、威胁信息、接口流量、连接信息、应用流量、用户流量、网站类型流量、VPN流量、在线用户等对象进行监控展示；需提供功能截图。 |
|  |  | 支持对CPU、内存、整机流量、新建、并发进行统计，展示CPU、内存实时利用率及其历史走势图； |
|  |  | 支持威胁可视化技术和流量可视化技术，可提供详细的分析展示图表；需提供功能截图。 |
|  |  | 支持主机威胁统计和展示，包括基于地理位置的威胁地图展示、基于威胁级别和威胁类型的统计分析、基于威胁事件源/目的主机的TOP10统计展示、基于具体威胁事件/威胁类型的TOP10统计展示等，统计展示的时间周期包括1小时/1天/7天/30天；需提供功能截图。 |
|  |  | 支持根据应用对通过的数据进行统计，包括应用总流量排名和各个应用的协议名称、总流量、上行流量、下行流量、流速； |
|  |  | 支持基于流量的TOP100用户和TOP100应用的流量曲线图，流量曲线图的统计周期包括小时、天、7天和30天；需提供功能截图。 |
|  |  | 系统统计详情。针对总流量、CPU、内存利用率，并发连接，新建连接，做72小时精细化曲线统计，曲线支持局部放大。 |
|  | ▲ | 日志服务 | 支持标准syslog协议 |
|  | ▲ | 支持日志合并功能，相同类型的日志支持合并操作，降低日志流量开销；需提供功能截图。 |
|  |  | 支持日志外发至多个SYSLOG服务器； |
|  |  | 支持流日志功能，将每一条数据流生命周期的各个业务模块的操作，整合为一条完整的日志进行展示；需提供功能截图。 |
|  | ▲ | 威胁情报防护服务 | 支持基于威胁情报云的动态防护功能，支持将用户对互联网的访问信息发送至威胁情报云进行实时情报查询及防护。提供配置界面及威胁情报云端界面截图； |
|  | ▲ | 威胁情报具备云端汇集实时热点高威胁情报数据，提供边界防御研判恶意可疑行为，区分高频随机性攻击与高危定向攻击，预判并阻断攻击威胁对业务的影响； |
|  | ▲ | 威胁情报类型包括可疑行为（垃圾邮件、网络爬虫、挖矿、主机扫描）、攻击威胁（网银大盗、爆破攻击、DDoS攻击、漏洞利用、Web漏洞攻击）、恶意站点（欺诈、赌博、钓鱼）、恶意软件（黑客工具、宏病毒、勒索软件、远控木马、网络蠕虫）、攻击组织（APT组织、僵尸网络C2、IoT攻击C2）、失陷主机（僵尸主机、IoT失陷主机）等； |
|  |  | 策略梳理服务 | 支持扩展集中策略分析模块；需提供功能截图。 |
|  |  | 支持集中对所有安全策略进行冗余分析，可分析出安全策略是否为不必要的冗余配置；需提供功能截图。 |
|  |  | 支持集中对所有安全策略进行收敛分析，也称宽松策略分析。能够支持查看任何一条宽松策略的流量详细信息；需提供功能截图。 |
|  |  | 支持集中对所有安全策略进行命中频率分析，辅助用户快速完成策略次序的调整，从而达到优化边界防护处理性能的目的；需提供功能截图。 |
|  |  | 支持集中对所有安全策略进行潜在冲突分析，辅助用户快速完成策略的调整，从而达到访问控制的目的；需提供功能截图。 |

#### 9、其它要求

1. “参数性质” 栏中划“▲”表示此参数为重要技术参数，其它为一般参数，不满足将扣除相应分数；
2. 需提供有关文件和资料，如产品彩页、检测报告、说明书等，否则为无效投标。
3. 采购人有权要求中标人在合同签署前对所有招标要求及投标响应逐一验证，并提供测试机，符合客户要求后才能执行合同流程，验证中发现虛假应标的行为将予以追究相关责任。

### 四、机房软、硬件产品维保

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **序号** | **名称** | **参考型号** | **现有配置情况** | **数量** | **维保内容** |
|  | 虚拟化服务器 | lenovo SR860 7X69 | XEON CPU\*2，300G硬盘\*3，双电源 | 9 | 整机及配件 |
|  | 存储交换机 | IBM SAN24B-5 | 24个16G接口，单电源 | 2 | 整机及配件 |
|  | 主存储 | lenovo V7000 | 3.84T硬盘\*6，2T硬盘\*12，双电源 | 3 | 整机及配件 |
|  | 主应用服务器1 | lenovo SR860 7X69 | XEON CPU\*2，300G硬盘\*3，双电源 | 4 | 整机及配件 |
|  | 存储扩展柜 | lenovo V7000 EXP | 4T硬盘\*12，双电源 | 1 | 整机及配件 |
|  | 原虚拟化服务器 | lenovo X3850X6 | XEON CPU\*2，600G硬盘\*2，双电源 | 2 | 整机及配件 |
|  | 原存储 | IBM V5000 | 4T硬盘\*12，双电源 | 2 | 整机及配件 |
|  | 存储交接机 | IBM 2498 B24 | 8个8G接口，单电源 | 1 | 整机及配件 |
|  | 服务器1 | dell R730 | XEON CPU，300G硬盘\*3，单电源 | 4 | 整机及配件 |
|  | 服务器2 | hp DL388G9 | Xeon CPU\*1，1T硬盘\*1，单电源 | 1 | 整机及配件 |
|  | 服务器3 | IBM X346 | XEON CPU\*1，146G硬盘\*1，单电源 | 1 | 整机及配件 |
|  | 服务器4 | IBM X3650 | XEON CPU\*2，146G硬盘\*1，单电源 | 1 | 整机及配件 |
|  | 服务器5 | IBM X3650M4 | XEON CPU\*2，500G硬盘\*4，单电源 | 1 | 整机及配件 |
|  | 服务器6 | IBM X3850M2 | XEON CPU\*2，146G硬盘\*2，双电源 | 1 | 整机及配件 |
|  | 服务器7 | IBM X3850X5 | XEON CPU\*2，300G硬盘\*4，双电源 | 4 | 整机及配件 |
|  | 服务器8 | lenovo RS260 | XEON CPU\*1，500G硬盘\*1，单电源 | 1 | 整机及配件 |
|  | 服务器9 | lenovo SR1507Y54 | XEON CPU\*1，2T硬盘\*1，单电源 | 1 | 整机及配件 |
|  | 服务器10 | lenovo X3650M4 | XEON CPU\*2，500G硬盘\*4，单电源 | 1 | 整机及配件 |
|  | 服务器11 | lenovo X3650M5 | XEON CPU\*2，600G硬盘\*5，双电源 | 4 | 整机及配件 |
|  | 服务器12 | 华为 2288HV5 | XEON CPU\*2，600G硬盘\*4，单电源 | 2 | 整机及配件 |
|  | 存储1 | dell MD3800i | 2T\*4硬盘，单电源 | 2 | 整机及配件 |
|  | 存储2 | 浪潮AS300N-M1 | 2T\*4硬盘，单电源 | 1 | 整机及配件 |
|  | 存储3 | 浪潮AS300N-M1 | 2T\*4硬盘，单电源 | 1 | 整机及配件 |
|  | 服务器13 | 浪潮NF8460M3 | XEON CPU\*1，146G硬盘\*2，单电源 | 1 | 整机及配件 |
|  | 服务器14 | 浪潮NF8460M3 | XEON CPU\*1，146G硬盘\*2，单电源 | 1 | 整机及配件 |
|  | 存储3 | 4T\*8 | 4T硬盘\*8 | 1 | 整机及配件 |
|  | 存储4 | IBM DS5020 | 600G\*12硬盘，双电源 | 1 | 整机及配件 |
|  | 存储5 | IBM EXP520 | 600G\*16硬盘，双电源 | 1 | 整机及配件 |
|  | 接入交换机1 | H3C S5560 | 24个千兆电接口，4个万兆光接口 | 2 | 整机及配件 |
|  | 接入交换机2 | H3C S6520 | 24个万兆光接口 | 2 | 整机及配件 |
|  | 备份一体机 | - | 2T\*4硬盘，单电源 | 1 | 整机及配件 |
|  | 虚拟化软件 | - | Vmware，9节点 | 1 | 应急与故障处理 |
|  | oracle RAC | - | HIS服务器2节点 | 1 | 应急与故障处理 |