**1.防火墙参数**

|  |  |
| --- | --- |
| **类别** | **招标要求** |
| 硬件结构 | ★标准1U机箱，≥12个10/100/1000BASE-T接口，硬件采用多核架构，具备多核多平台并行TOS安全操作系统证书， |
| 性能指标 | ★网络吞吐率≥600M，最大并发连接数≥100万 |
| 系统要求 | 网络特性 | ★支持路由、透明、混合与虚拟线部署 ；（提供功能界面截图） |
| 支持多链路接入环境下的出站多运营商智能选路与入站智能DNS； |
| ★支持服务器负载均衡功能，并至少提供10种以上服务器负载均衡算法 ；（提供功能界面截图） |
| 基础安全 | 能够基于访问控制策略对最大并发连接数限制； |
| 支持在WEB界面中查看每条策略所匹配的当前会话、历史会话与报文统计信息； |
| 支持免客户端方式实现跨越路由（或其他三层设备）进行IP/MAC绑定功能； |
| 应用安全 | 应用识别 | 支持P2P（下载、音频、视频）、即时通讯、语音电话、网上银行、电子商务、财经软件、网络游戏、社交网络、网页应用（视频、音频、网盘、web邮箱等等）、远程控制、数据库等多种类型主流应用识别和控制； |
| ★支持加密流量识别，如HTTPS流量、BT加密流量、迅雷加密流量、网络视频加密流量、Skype加密流量等等 ；（提供功能界面截图） |
| 内容过滤 | 支持对URL最大长度进行限制以及对FTP命令进行过滤，包括上传、下载、追加、删除文件、重命名、列表、创建目录、删除目录等； |
| ★内置500万以URL分类地址库，支持挂马网站过滤，且内置挂马网站特征库 ；（提供功能界面截图） |
| 支持HTTP、FTP、Telnet、SMTP、POP3、IMAP等协议进行登陆标题信息替换； |
| 病毒防护 | ★内嵌快速扫描、深度扫描双引擎杀毒技术，并可以针对HTTP、SMTP、POP3、FTP和IMAP协议选择不同的扫描引擎；每种扫描引擎具有独立的病毒库，病毒库总数大于700万；（提供功能界面截图）  |
| 采用国际、国内知名品牌病毒库，病毒库提供商应通过VB100认证；厂商防病毒技术或防病毒产品的病毒检测率大于98%； |
| 入侵防御 | ★攻击规则库数量大于3500条，同时支持自定义攻击检测规则与自定义规则执行动作；（提供功能界面截图）  |
| 为适应不同网络及应用环境，引擎检测模式可选择智能检测或深度检测，数据处理模式可选择应用优先或安全优先，并能够在丢弃报文时发送TCP reset命令； |
| APT防御 | 未知威胁检测 | 不依赖于攻击、恶意代码等特征库进行检测，通过沙箱技术对于未知漏洞攻击（0day/1day漏洞）、木马、病毒具有检测能力（提供功能界面）； |
| ★能够生成详尽的未知威胁分析报告，包括文件的静态基本信息、危险行为、文件操作和进程执行等信息；（提供功能界面截图） |
| 智能网管 | 健康体检 | 支持智能策略优化、策略合规性检测与策略冗余检测； |
| 支持设备健康体检功能，通过结合内置的健康评分体系，对设备的健康情况进行综合评定，并以“一键式健康体检评分”和“多视角体检分析报告”的形式进行展现； |
| 风险评估 | 内置安全趋势风险识别分析模型，有效实现对设备的安全趋势进行实时跟踪；支持风险评估关联日志分析，能够通过FW、AV、IPS、URL、APT日志有效评估网络风险状况，深度分析网络威胁构成； |
| 支持全网风险评估：通过全网可视化功能（设备物理资源、设备运行、网络流量、设备安全状况、应用、用户行为等）进行全网风险评估，同时支持将可视化结果通过柱状图、折线图、点状图和饼状图等方式进行展现； |
| VPN模块 | IPSEC VPN | 支持DES/3DES/AES等标准加密算法，支持MD5/SHA1标准HASH算法，支持DH GROUP1/2/5，RSA 1024/2048非对称算法； |
| SSL VPN | 支持资源自动打开、资源连接隐藏、资源与特定应用程序关联；支持用户设定代理服务器信息（提供功能界面）； |
| ★支持Windows XP、2003、2008、Vista、Win7、Win8及Linux系统PC；支持Windows Mobile、Android智能终端的全网接入模式（非PPTP方式）；（提供功能界面截图） |
| 资质要求 | ★产品资质 | 具备《计算机信息系统安全专用产品销售许可证》（三级）；ISCCC产品认证证书(三级)；涉密检测证书；具备国家密码管理局商用密码检测中心-防火墙产品密码检测证书；具备国家信息技术产品安全评测证书EAL3+认证；自主原创产品测评证书；电信设备进网许可证；《多核多平台并行安全TOS操作系统》，提供以上资质文件 |
| ★制造厂商资质 | 信息安全服务资质认证－安全工程类服务资质（二级）；国家信息安全测评信息安全服务资质（安全开发类一级）；信息安全服务资质认证－信息系统安全集成服务资质（一级）；ISO27001信息安全管理体系认证证书；ISO20000信息技术服务管理体系认证证书；环境管理体系14000认证；《网络安全应急服务支撑单位证书》（国家级）；《通信行业质量管理体系认证证书》（TL9000证书）；中国国家漏洞库一级支持单位资质；信息安全风险评估服务资质（一级）；《CMMI 3级》；信息安全应急处理服务资质（一级）；涉及国家秘密的计算机信息系统集成资质（甲)；提供以上资质文件 |
| ★产品成熟度 | 为保证产品的成熟度和可靠性，要求防火墙产品提供CCID或IDC连续15年市场排名前三的证明文件。 |
| ★技术服务要求 | 原厂负责实施人员不得低于3人，同时具有国家信息安全测评中心CISP证书，需提供湖北本地半年以上社保证明文件；（提供有效证明的复印件） |
| 厂商具备专业的攻防研究团队，能够对安全漏洞进行持续的挖掘与跟踪。2016年向CNVD(国家信息安全漏洞共享平台)贡献的漏洞数量排名不低于前三名。（提供CNVD官网截图证明） |
| 其他 | 提供原厂针对本项目的“项目授权函”原件和三年的售后服务承诺函； |

**2.防病毒网关**

|  |  |
| --- | --- |
| **类别** | **招标参数** |
| 硬件要求 | 标准1U机箱，配置为6个10/100/1000BASE-T接口（默认电口具有一组BYPASS接口），1个RJ-45串口 |
| 性能参数 | 整机吞吐率：≥1Gbps，最大并发连接数：≥140W，病毒检测吞吐率：≥100Mbps  |
| 防病毒引擎 | ★内嵌双引擎杀毒技术，可单独采用流杀毒（快速扫描）引擎或文件型杀毒（深度扫描）引擎，也可同时支持两种杀毒引擎，能够根据不同的被检测协议采用不同杀毒引擎（提供产品功能截图）；能够防御病毒、木马、蠕虫，且支持对压缩数据、加壳病毒的查杀； ★能够支持对SMTP、POP3、IMAP、HTTP和FTP协议进行病毒扫描和过滤，有效地防止可能的病毒威胁；（提供产品功能截图）支持病毒隔离功能，管理员可以方便的管理隔离区，可以选择把隔离区的内容发送给管理员或者删除；可以实时检测到日益泛滥的蠕虫攻击，并对其进行实时阻断，从而有效防止内部网络因遭受蠕虫攻击而陷于瘫痪；要求支持信任站点功能，网关针对信任站点不做病毒扫描，以降低病毒扫描引擎的负担；★支持IPv4和IPv6双栈协议的病毒扫描和过滤；（提供产品功能截图）★支持智能检测应用协议的病毒行为，采用智能方式准确扫描常用协议任意端口的病毒传输行为，而非通过传统手动配置协议端口绑定形式进行病毒扫描；（提供产品功能截图）★支持多接口旁路的病毒传输监听检测方式，可并行监听并检测多个网段内的病毒传输行为，用于高吞吐量、高可靠性要求的旁路应用环境；（提供产品功能截图）★支持通过采用java的 Commons FileUpload或其他类似控件的OA、CRM及其他基于WEB的应用系统（包括WEBMAIL）上传文件时的病毒查杀；（要求测试）★要求提供病毒检测率不低于98%的第三方证明；（提供产品功能截图） |
| 病毒库 | ★采用国际国内知名主流品牌病毒库，并提供两家以上专业病毒厂商的授权证明文件，病毒库提供商应通过VB100认证（需能够在病毒库提供商的网站首页可查）；★要求每种扫描引擎具有独立的病毒库（提供截图），病毒库总数大于1000万（提供产品功能截图）；★要求具有独立的蠕虫防护规则库，并可通过手动或自动方式进行升级；（提供产品功能截图） |
| 内容过滤 | 支持对数据内容进行检查，可以采用关键字过滤、URL过滤等方式来阻止非法数据进入内部网络，并且能够针对“ActiveX”、“Java Applets”及“Script”等控件实施拦截；★要求能够根据文件内容识别文件真实类型，有效的阻断非法类型的文件进入企业网络，能够防止通过修改文件扩展名的方式逃避过滤；（提供产品功能截图） |
| 反垃圾邮件 | 采用邮件地址与IP地址的黑、白名单技术实时检测垃圾邮件并阻止其进入企业网络，为企业节省宝贵的带宽； |
| 维护与管理 | 提供完整的病毒日志、访问日志和系统日志等记录，并可根据日志数据生成多种格式的统计图形化统计报表；提供强大的监控功能，可以监控系统资源、网络流量、当前会话数、当前病毒扫描信息等；报警配置用于当病毒突然爆发时，可向网络管理员发送报警信息，需支持邮件报警、声音报警、SNMP等报警方式；★要求具有配置文件自动定时上传到指定外部服务器功能；（提供产品功能截图） |
| ★资质要求 | 要求设备为专业的防病毒网关产品，非防火墙、UTM、上网行为管理等加配模块的产品；要求资质必须为防病毒网关的专用资质，非UTM或防火墙资质；公安部-计算机信息系统安全专用产品销售许可证（增强级）；病毒过滤网关IPv6Ready2资质认证；国家版权局-计算机软件著作权登记证书；国家版权局-多核多平台并行TOS安全操作系统；  |
| ★制造厂商资质 | 信息安全服务资质认证－安全工程类服务资质（二级）；国家信息安全测评信息安全服务资质（安全开发类一级）；信息安全服务资质认证－信息系统安全集成服务资质（一级）；ISO27001信息安全管理体系认证证书；ISO20000信息技术服务管理体系认证证书；环境管理体系14000认证；《网络安全应急服务支撑单位证书》（国家级）；《通信行业质量管理体系认证证书》（TL9000证书）；中国国家漏洞库一级支持单位资质；信息安全风险评估服务资质（一级）；《CMMI 3级》；信息安全应急处理服务资质（一级）；涉及国家秘密的计算机信息系统集成资质（甲)；提供以上资质文件 |
| ★技术服务要求 | 原厂负责实施人员不得低于3人，同时具有国家信息安全测评中心CISP证书，需提供本地半年以上社保证明文件；（提供有效证明的复印件） |
| 厂商具备专业的攻防研究团队，能够对安全漏洞进行持续的挖掘与跟踪。2016年向CNVD(国家信息安全漏洞共享平台)贡献的漏洞数量排名不低于前三名。（提供CNVD官网截图证明） |
| ★ | 提供原厂针对本项目的“项目授权函”原件和三年的售后服务承诺函； |

**3.终端管理系统**

|  |  |
| --- | --- |
| **类别** | **招标参数** |
| 功能指标 | 通用指标 | 支持B/S模式管理支持SSL加密模式访问全部功能提供联机帮助文档服务器可以支持32/64位windows Server操作系统数据库支持Oracle9i及以上、SQLServer 2005及以上WSUS支持2.0及以上 |
| 资产管理 | 资产分组管理、资产增加、修改和删除资产组信息包括：名称、别名、描述、资产数、所有者、创建者、创建时间信息等支持资产组的查看方式：按漏洞列表、按资产类型统计信息等资产信息包括：基本信息，用户列表，资产变更信息，类型列表，漏洞列表，补丁列表，接口列表，硬件信息列表，软件信息列表等支持资产的查看方式：按资产使用人、按物理区域组、按用户组、按漏洞组、按补丁组、按资产基本信息等支持资产的查询方式：按用户基本信息、按资产基本信息、按漏洞信息、按补丁信息等支持资产的导入和导出支持资产组和资产的移动 |
| 系统监控 | 总报警数按级别统计个数可以监控Agent版本号主机端口使用情况（包括占用端口的进程、协议和IP地址等信息）进程情况（当前运行进程列表、各进程的CPU使用率、内存使用量、线程数等信息，可以停止部分进程）软件信息（已安装的软件名称和版本等信息）硬件信息（包括主机各部分硬件的名称、厂商等信息）性能信息（包括CPU使用率、内存使用率和磁盘使用率）补丁信息（已安装补丁和未安装的补丁信息，手动安装补丁）漏洞信息（包括漏洞的危险级别及其对应的补丁）策略信息（监视已经下发到Agent主机上的策略类型和下发时间等信息）查看Agent资产信息、报警信息、获取本地日志及远程协助 |
| 补丁管理 | 按操作系统类型和资产类型进行列表和柱状图统计支持对补丁文件分类，补丁分为已验证、未验证和正在验证三种类型，“已验证”类中又分为安全更新程序、关键更新程序、更新程序、更新程序集、更新包和工具支持对补丁进行验证支持补丁下发和卸载 |
| ★非法内联 | 支持定义合法IP，支持手工输入和txt/csv文件导入（提供功能界面截图）可监视指定网段内所有在线IP，列表显示是否合法、Agent是否安装、杀毒软件是否安装（提供功能界面截图）可统计在线IP数、合法IP数、在线Agent数、安装Agent数、安装杀毒软件数（提供功能界面截图）可按IP地址、IP是否合法、是否安装Agent、是否安装杀毒软件等内容进行查询（提供功能界面截图）使用ARP欺骗方式阻断非法接入的主机或设备，可定义阻断的IP或网段（提供功能界面截图）发现非法IP时可进行报警、Agent提示、阻断（可自定义阻断时间）或重启Agent主机（支持延时重启）（提供功能界面截图） |
| 策略管理 | 所有策略均具备的功能，按照策略名称进行管理。对每条策略可以定义违规危险级别、报警处理方式（记录到本地和上传到服务器）、报警上报时间间隔、备注信息。支持策略下发到已安装Agent的主机。支持已下发策略的启用、禁用。可按照主机IP或IP范围查询已应用的策略。支持策略组定义和下发。支持的策略类型（以下“主机”如无特殊说明均指安装了Agent的主机）：支持文件监控策略。对指定文件夹下的文件和文件夹的创建、修改、删除、重命名操作可以有选择地禁止支持针对终端存储的word、pdf、Excel、文本文件等进行全盘关键字检查，对含有制定关键字的文档进行禁止发送、禁止打印、禁止拷贝等管控，同时将文档信息上报服务器。支持复合关键字检索，支持关键字出现频率制定。支持指定主机的补丁检测时间（主机启动时检测或间隔一定时间定时检测）、下载的补丁类型（安全更新程序、关键更新程序、工具、更新程序、更新程序集和更新包）、下载的补丁级别、补丁安装前提示、安装后重启支持设备监控策略。（可以对主机的以下设备进行启用禁用操作：光驱、软驱、USB设备、打印机、调制解调器、串口、并口、1394控制器、红外设备、蓝牙设备、PCMCIA卡、SCSI和RAID控制器、磁带机、图形处理设备、无线网卡、智能卡、多媒体设备，支持设备白名单。）支持打印监控策略。三种选项：禁止、允许、允许并报警支持拨号监控策略。三种选项：禁止、允许、允许并报警支持外存监控策略。对光盘和软盘可以使用三种选项：禁止、允许、允许并报警。支持对移动存储设备采用标签式管理，可以定义禁用、启用只读、启用（只读\_运行）和启用读写、启用（读写\_运行）五种操作支持对访问移动存储设备时进行审计，支持违规时在主机提示用户支持硬件监视策略。可在主机硬件变化时报警支持外联监控策略。支持定义内网IP范围、检测周期、外网检测地址、违规处理方式（不处理、重启、断网、提示）支持HTTP访问策略。可定义信任站点列表、限制站点列表，可对主机访问的站点进行阻断、报警、记录日志操作支持共享监视策略。可在共享被创建、修改、删除或重命名时在主机弹出提示支持流量控制策略。可控制Agent进行补丁和软件下发时的通信流量，可定义最大、最小传输速率、断点续传间隔时间支持流量统计策略。可定义主机的出站、入站最大流量，可在超出范围后阻断网络，可定义阻断时间支持进程监视策略。可定义进程黑、白名单，定义单个进程的内存、CPU阀值，超过后将报警。白名单指定进程未启动时可阻断网络，黑名单中的进程可自动中止支持端口监视策略。支持定义端口黑、白名单，白名单中的端口未开放或者黑名单中的端口已开放均会产生报警支持软件监视策略。当系统中新安装、卸载软件时可报警，并且可以禁用“添加或删除程序”面板，限制软件安装（包括绿色软件）支持系统性能策略。支持内存和CPU使用率上限和持续时间定义，当超过上限和持续时间时报警。支持监控硬盘剩余空间，当低于下限时报警支持网络配置监控策略。可禁止用户修改网络参数，禁止用户使用多网卡。违规时可以断开网络，可自定义断开时间支持主机防火墙策略。支持定义进程通讯规则，可指定规则名称、进程名称、通讯协议、本地端口列表、远程IP和端口列表、数据流向（传入、传出和双向）、处理方式（阻断/放行、记录日志、报警）支持设置内外网切换规则，主机可选择使用内网或外网支持设置包过滤规则，定义默认规则（是否允许网络共享、是否允许TCP/UDP通讯）、规则名称、本地IP和端口列表、远程IP和端口列表、数据流向（传入、传出和双向）、处理方式（阻断/放行、记录日志、报警） |
| ★网络准入 | 支持与产品防火墙联动，可支持多台（提供功能界面截图）支持802.1x认证支持产品防护墙+交换机复合准入 |
| ★综合查询 | 支持Agent查询、策略下发查询、补丁下发查询、事件查询、杀毒软件查询（提供功能界面截图） |
| 系统维护 | 支持对Agent进行查看、暂停、管理插件、设置报警、群发消息等操作支持对Agent的远程卸载、升级、关联支持对控制器的查看、暂停、参数设置支持控制器远程升级支持对移动存储设备进行标签式管理，支持移动存储设备的身份识别和验证支持Agent安装包服务器直接生成，并且在首页上提供下载链接支持事件信息手动清理 |
| ★软件分发 | 支持FTP方式的软件分发，可指定下发时间、分发后的处理方式（不安装、立即执行、强制安装）（提供功能界面截图）可根据Agent的IP地址、下发时间、软件名称、下发状态、安装状态等进行查询（提供功能界面截图） |
| ★报表功能 | 提供多种报表模版（提供功能界面截图）支持表格及多种图形表现形式（柱状图、饼图、曲线图）（提供功能界面截图） |
| 性能指标 | ★并发管理Agent数量 | 服务器硬件配置越高，并发管理的数量越多，没有具体测试数据服务器软件有上限：系统最多添加2000个，同时在线最多1000个（提供功能界面截图） |
| ★资质要求 | 计算机信息系统安全专用产品销售许可证；涉密信息系统产品检测证书；信息安全产品认证证书（C+级）；计算机软件著作权登记证书；国家信息安全测评信息技术产品安全测评证书（EAL3级）；软件产品登记证书 |
| ★制造厂商资质 | 信息安全服务资质认证－安全工程类服务资质（二级）；国家信息安全测评信息安全服务资质（安全开发类一级）；信息安全服务资质认证－信息系统安全集成服务资质（一级）；ISO27001信息安全管理体系认证证书；ISO20000信息技术服务管理体系认证证书；环境管理体系14000认证；《网络安全应急服务支撑单位证书》（国家级）；《通信行业质量管理体系认证证书》（TL9000证书）；；中国国家漏洞库一级支持单位资质；信息安全风险评估服务资质（一级）；《CMMI 3级》；信息安全应急处理服务资质（一级）；涉及国家秘密的计算机信息系统集成资质（甲)；提供以上资质文件 |
| ★技术服务要求 | 原厂负责实施人员不得低于3人，同时具有国家信息安全测评中心CISP证书，需提供本地半年以上社保证明文件；（提供有效证明的复印件） |
| 厂商具备专业的攻防研究团队，能够对安全漏洞进行持续的挖掘与跟踪。2016年向CNVD(国家信息安全漏洞共享平台)贡献的漏洞数量排名不低于前三名。（提供CNVD官网截图证明） |
| 为保证服务的及时可靠性，厂商须在湖北本地有常驻分支机构，非办事处，提供本地营业执照复印件。 |
| ★其他 | 提供原厂针对本项目的“项目授权函”原件和三年的售后服务承诺函； |

**4.杀毒软件**

|  |  |  |
| --- | --- | --- |
| **类别** | **指标项** | **指标要求** |
| 安装部署 | 支持B/S管理架构 | 管理端支持全中文界面，纯B/S架构，无需安装客户端软件。管理员只需通过浏览器登陆控制中心，即可对虚拟机进行管理。本次要求提供110个客户端杀毒和5个服务器端杀毒许可。 |
| 轻量级客户端安装 | ★（截图）客户端资源占用应小于50MB，有效节省终端资源使用率。 |
| 操作系统支持 | 至少支持WindowsXP、Windows 7、Windows 8、Windows 10等32位/64位操作系统，同时并支持Windows2003、Windows2008、Windows2012、Windows2016等32位/64位服务器操作系统。 |
| 管理控制 | 可视化展示 | ★（截图）支持全网威胁统计分析管理控制台可直观的展示病毒趋势统计、终端信息、病毒类型排行、病毒排行、终端危险排行等统计情况。并随时对网络中病毒发生的情况进行查询统计，能按时间、按IP地址、机器名、按病毒名称、病毒类型进行展示。 |
| 终端管理 | ★（截图）管理控制台支持实时显示客户端的状态，包括机器名称、IP地址、mac地址、操作系统、显卡信息、内存大小、连接状态、监控状态、当前版本信息和物理位置等信息。 |
| 支持对防病毒客户端进行分组，根据不同的组别可以设定不同的策略和执行不同的任务。 |
| 支持对全网进行集中的管理和任务下发，可以通过控制台立即给客户端发送命令，包括立即杀毒、立即升级、关机、重启、显示消息等，而不需要通过建立策略方式实现，从而简化和方便了管理员的管理。 |
| 管理控制台支持通知客户端立即升级、强制更新、客户端主动升级等更新方式。 |
| 权限控制 | ★（截图）支持客户端防删功能，能够防止客户端在未经管理员允许情况下强行卸载。 |
| 支持客户端未开机的全网查杀策略设置，在客户端下次启动时策略补做功能。 |
| 支持分级管理及多管理员权限划分，如：超级管理员，操作管理员。同时管理控制台支持自定义管理员权限设定。 |
| 行为审计 | 管理控制台支持对客户端的系统操作行为进行记录功能，便于管理员对用户操作审查和分析 |
| 统计分析 | 支持客户端威胁日志信息上报统计功能，包含终端危险排行统计、防御类型分布统计、病毒类型分布统计、病毒排行统计等，支持图表显示。 |
| 报表功能 | ★（截图）报表内容必须包括御类型分析、病毒类型分析、病毒排行、终端杀毒排行、病毒趋势统计、黑客拦截、对外攻击分析。支持威胁Top10、Top20、Top30排行。 |
| 报表应该可以通过表格以及图形方式进行展现，支持将生成的报表以Excel、word、HTML、PDF等通用格式输出；。 |
| 支持按日、周、月定期推送报表功能。 |
| 策略管理 | ★（截图）控制台支持恶意网站拦截、浏览器保护、恶意行为、文件保护、下载保护、黑客拦截、系统加固、U盘防护、邮件监控、白名单等策略下发。 |
| ★（截图）管理控制台支持预制策略功能，保障新安装客户端自动应用组策略。 |
| 客户端防护 | 病毒查杀 | 至少支持对终端电脑内部文件进行全盘扫描、快速扫描，自定义扫描三种扫描能力。并具备空闲查杀、异步查杀、断点查杀、后台查杀等功能 |
| 支持扫描和清除各种广告软件、恶意插件、隐蔽软件、黑客工具、风险程序等等。 |
| 支持Office/IE/Lotus Notes等嵌入杀毒；支持用户添加嵌入杀毒的应用程序；支持MSN Messenger、AOL Messenger、FlashGet、NetAnts、NetVampire、WinZip、WellGet、WinRAR等工具的嵌入式杀毒功能 |
| ★（截图）支持病毒自动隔离功能，对于暂时无法清除的被感染文件或者可疑文件，防病毒软件的客户端能自动将其隔离到本地隔离区。 |
| 支持未知病毒、恶意代码的防范能力，支持基于行为的检测和防护技术：针对未知恶意威胁具有行为评分能力，智能识别蠕虫木马，无需提示用户操作判断。 |
| 支持注册表病毒、内存或服务类病毒的查杀，提高终端安全防护等级，对已经运行的病毒进程可以执行关闭。 |
| 支持病毒查杀时目录排出功能。 |
| 安全检测 | 支持U盘扫描检查功能，防止病毒通过U盘在终端传播有效保护终端不受病毒侵扰。 |
| 支持对网页进行病毒、木马进行监测及防护，对可能产生威胁的网页进行提示或屏蔽。 |
| 支持客户端对外攻击检测，防止用户终端感染病毒后的对外对外攻击行为，避免用户的利益受到损害。 |
| 实时监控 | 能够实时监控和清除来自各种途径的病毒、木马、恶意程序。 |
| 邮件监控 | 支持对终端内文件、邮件、网页一体化实时监控，防止病毒运行； |
| ★（截图）支持基于SMTP/POP3协议的邮件监控，包括如：Outlook、Outlook Express、foxmail、DreamMail等邮件客户端的防（杀）病毒。 |
| 威胁情报 | ★（截图）支持可疑文件上报功能，如果用户觉得某个文件比较可疑，可将此文件上报给病毒管控中心进行检查分析和处理，并将情报全网共享。 |
| 其他 | ★产品资质 | 具有《计算机信息系统安全专用产品销售许可证》、《计算机软件著作权登记证》提供证书复印件证明。 |
| ★制造厂商资质 | 信息安全服务资质认证－安全工程类服务资质（二级）；国家信息安全测评信息安全服务资质（安全开发类一级）；信息安全服务资质认证－信息系统安全集成服务资质（一级）；ISO27001信息安全管理体系认证证书；ISO20000信息技术服务管理体系认证证书；环境管理体系14000认证；《网络安全应急服务支撑单位证书》（国家级）；《通信行业质量管理体系认证证书》（TL9000证书）；中国国家漏洞库一级支持单位资质；信息安全风险评估服务资质（一级）；《CMMI 3级》；信息安全应急处理服务资质（一级）；涉及国家秘密的计算机信息系统集成资质（甲)；提供以上资质文件 |
| ★技术服务要求 | 原厂负责实施人员不得低于3人，同时具有国家信息安全测评中心CISP证书，需提供湖北本地半年以上社保证明文件；（提供有效证明的复印件） |
| 厂商具备专业的攻防研究团队，能够对安全漏洞进行持续的挖掘与跟踪。2016年向CNVD(国家信息安全漏洞共享平台)贡献的漏洞数量排名不低于前三名。（提供CNVD官网截图证明） |
| 为保证服务的及时可靠性，厂商须在湖北本地有常驻分支机构，非办事处，提供本地营业执照复印件。 |
| ★其他 | 提供原厂针对本项目的“项目授权函”原件和三年的售后服务承诺函； |

**5.核心交换机**

|  |  |
| --- | --- |
| **功能及技术指标** | **参数要求** |
| ★整体要求 | 机箱型插槽式交换机 |
| 业务插槽数≥3 |
| 交换架构 | 机框式模块化三层交换机架构 |
| ★整机性能 | 交换容量≥15Tbps，包转发率≥7000Mpps |
| 常规功能及性能 | 整机ARP表项≥170K，MAC地址表容量≥100万，ACL表项容量≥64K，满足大容量访问要求 |
| 支持ARP Proxy、支持DHCP Relay、支持DHCP Server、支持VRRP、支持URPF |
| 支持静态路由、RIP V1/V2、OSPF、BGP，提供策略路由功能。 |
| 支持OSPF/IS*-*IS/BGP GR，虚拟路由冗余协议（VRRP）、支持双引擎负载分担；提供软件热补丁技术，实现设备软件完全平滑升级； |
| 虚拟化特性 | 支持多台交换机虚拟堆叠技术，控制平面与数据平面均可表现为1台逻辑设备，支持多台设备单一IP地址管理，跨设备的链路聚合，分布式的路由冗余 |
| 接口 | 支持千兆电口、千兆光口、万兆光接口 |
| 多业务扩展能力 | 支持防火墙业务板卡，对DoS/DDoS攻击、ARP欺骗攻击、TCP报文标志位不合法攻击、超大ICMP报文攻击等威胁的防范，集成IPSec、L2TP、GRE等多种成熟VPN接入技术，保证移动用户、合作伙伴和分支机构安全、便捷的远程接入，提供官网订购信息截图及链接； |
| 支持无线业务板卡，可对传统802.11a/b/g/n AP管理，支持集中式转发和分布式转发，用户根据业务需要和网络实际情况可以灵活设置转发方式 |
| ★资质证明 | 可提供近3年任一年份由第三方权威机构IDC发布的关于中国国内交换机市场（非运营商市场）排名前3名的证明文件复印件并加盖制造商鲜章； |
| 为保障产品质量，设备制造厂商需具备科学、系统的知识产权管理体系，以支撑企业的技术创新能力，产品制造商需提供知识产权管理体系认证证书复印件并加盖制造商鲜章 |
| 为保障产品质量，生产厂商国内研发机构需通过CMMI4或以上认证，提供在有效期内的证书复印件并加盖制造商鲜章 |
| 为保护机房工作的维护人员身体健康，本次投标产品需通过QC08000有害物质过程管理体系认证，需提供证书复印件并加盖制造商鲜章 |
| ★配置要求 | 本次配置共1台，单台详细配置如下： |
| 单台配置主控、冗余交流电源；单台配置千兆电口≥24个,4\*千兆单模光纤模块 |

**6.接入交换机**

|  |  |
| --- | --- |
| **功能及技术指标** | **参数要求** |
| ★品牌 | 与内网核心交换机同一品牌 |
| ★整体要求 | 交换容量≥335Gbps，转发性能≥65Mpps |
| 千兆电接口数量≥24个 |
| 非复用千兆光接口≥4个 |
| VLAN特性 | 支持基于端口的VLAN，支持基于协议的VLAN,支持基于MAC的VLAN； |
| 路由协议 | 支持静态路由、RIP、OSPF等路由协议 |
| ★功耗 | 整机满负荷功耗≤25W |
| 生成树 | 支持STP/RSTP/MSTP协议； |
| DHCP | 支持DHCP Server |
| 支持DHCP Snooping，防止欺骗的DHCP服务器； |
| 资质认证 | 提供工信部入网证 |

**7. 内部网络整理及线路规范**

 含全院内、外网线路整理、IP规范、机房网络线路整理、标号(含电话线路)等相应工作(含耗材)。