第三包 技术要求与参数

技术要求与参数
一、防火墙 （2套） 1.要求设备最大吞吐量不低于25Gbps，IPS吞吐量不低于7.5Gbps，AV吞吐量不低于7.5Gbps，最大并发连接数不低于700万，每秒新建连接数不低于55万，内置双电源，内存不低于16GB，硬盘不低于2TB。最低标配16个千兆电口（含2组电口Bypass），4个千兆光口，4个万兆光口；支持不少于2个接口扩展槽。 2.要求支持路由模式、交换模式、旁路模式、虚拟网线工作模式；部署模式切换无需重启设备。 3.支持基于时间段的SNAT、DNAT规则；SNAT转换地址池支持黑洞路由，支持SNAT的源端口不转换模式；DNAT-双向NAT模式支持基于地址池的源转换方式，DNAT的健康探测支持的协议TCP和ICMP；NAT66的SANT支持前缀转换方式。 4.要求支持IPSec VPN及支持SSL VPN功能。SSL VPN的PC客户端支持Windows、macOS等操作系统。 5.▲要求系统定义超过20万条资产指纹库，可识别的主机资产类型包括但不限于通用主机、移动电话、防火墙、网络摄像机、温湿度变送器、呼叫中心、云安全、Windows，Linux，MAC OS，Android，IOS等，WEB组件、WEB中间件等WEB应用，Oracle、Hive等数据库等。提供此功能证明材料。 6.▲要求支持基于主机、软件维度的资产发现，可识别资产所属厂商、IPv4地址、IPv6地址、MAC地址、资产类型、操作系统、用户、位置、价值、风险、弱密码、软件等信息；可识别软件IP地址、软件类型、软件名称、版本、Banner、协议、端口、用户等信息。提供此功能证明材料。 7.具备漏洞扫描功能，设备内置的默认模板以及自定义模板进行漏洞扫描，可扫描出漏洞名称、漏洞级别、漏洞描述、CVE-ID、CNNVD-ID等信息；支持查看资产关联的漏洞信息，并跳转到详情。 8.▲要求系统预定义超过11000条主流攻击规则，包含对应IPS规则的级别、防护对象、操作

系统、CVE 编号等详细信息。提供此功能证明材料。

9.▲要求支持独立的 Web 防护模块，系统定义超过 4500 条 WAF 规则防护功能，支持常规 HTTP 漏洞、SQL 注入、组件、CMS、WebShell 和 XSS 等类型的 Web 防护；支持 HTTP 协议的 URL、Method、Referer、User-Agent、Cookie、URL-args 等字段的等于、不等于、包含、不包含、正则等多种匹配方式的访问控制。提供此功能证明材料。

10.要求支持 Telnet、FTP、IMAP、POP3、SMTP、HTTP 协议的弱密码防护，支持预定义弱密码规则和自定义弱密码防护。

11.要求支持针对威胁事件采取操作，支持将源 IP 或目的 IP 加入黑名单（时长可选，永久、24 小时）；支持手动忽略选中的威胁事件，忽略后，相关威胁情报不再触发威胁事件；支持根据时间段导出威胁事件日志；支持威胁事件统计图形化分类展示，支持统计 Top10 的源 IP 及其威胁事件数量。

12.威胁情报检测能力：要求支持检测 C&C、勒索软件、僵尸网络、挖矿软件、矿池地址等安全攻击类型。

13.▲要求设备具备中国信息安全测评中心颁发的《国家信息安全测评信息技术产品安全测评证书》（万兆）EAL4+。提供证书复印件或扫描件。

二、堡垒机（1 套）

1.要求设备最低配置 6*GE 电口,硬盘容量不低于 2T。要求所需授权资产不低于 100 个，设备并发字符连接不低于 100 个，并发图形连接不低于 20 个。

2.要求支持按部门组织架构（至少 10 个层级的部门）管理用户数据、资产数据、授权数据、审计数据，且数据相互隔离；要求可按部门层级分别设定各部门不同权限的管理员，如部门内的运维管理员、审计管理员、系统管理员等。每个部门管理员仅可管理本部门及下级部门的相关配置。

3.支持标准化对接 CAS、JWT、SAML2、OAuth2 单点登录认证，且支持配置是否自动创建堡垒机中不存在用户，提供此功能证明材料。

4.▲要求支持标准适配多个云环境，包括阿里云、华为云、百度云、亚马逊云、腾讯云、Ucloud 等，支持同步云上主机信息至堡垒机。提供此功能证明材料。

5.▲要求支持自动收集设备 IP、运维协议、端口号、账号、密码、与用户的权限关系，可自动完成授权，提供此功能证明材料。

6.▲要求持对 Web 应用的自动改密功能，并且支持随堡垒机提供的改密插件录制向导，通过改密插件自动生成 web 应用的改密脚本。提供此功能证明材料。

7.▲要求支持对运维操作会话的在线监控、实时阻断；支持录像慢速/快速回放（最慢 0.5 倍速/最快 64 倍速）、支持记录起止时间、来源用户、来源 IP、目标设备、协议/应用类型、命令记录、操作内容（如对文件的上传、下载、删除、修改等操作等）的详细行为日志。提供此功能证明材料。

三、防病毒系统（1 套）

1. 要求提供防病毒服务1套，PC端配置不低于150个,服务器端配置不低于13个。提供3年软件服务使用许可、特征库升级、技术支持服务。

2. ▲要求支持可视化态势大屏展示，包括终端安全管控大屏和安全概况大屏，安全概况展示内容包括防护概况、检测概况、入侵检测概况、防护风险趋势、安全动态；终端管控包括终端状态、分组分类、版本状态、安装量、防护率、在线率等。提供此功能证明材料。

3. 要求支持展示当前待处理的高危风险信息，包括弱口令、待处理病毒、待处理漏洞数据，支持一键跳转到对应处理页面。

4. 要求支持自动收集终端资产信息，包括：计算机名称、内核版本、操作系统、处理器、主板、内存、硬盘、显卡等基础信息及监听端口、运行程序、账号、安装软件、Web框架、Web服务、数据库、Web应用、注册表启动项、系统安装包、JAR包、计划任务、环境变量、Windows证书等详细信息。

5. 内置在线沙箱，可对文件进行沙箱引擎分析、杀毒引擎分析、威胁情报分析，包含静态检测、样本行为分析、攻击矩阵、进程树展示，可在线预览分析结果并支持分析报告下载。

6. ▲要求支持对CPU、内存、磁盘使用、网络IO达到配置阈值时告警。支持对CPU、内存达到一定阈值时客户端自动进行熔断，提供此功能证明材料。

7.▲要求提供专门的针对未知勒索病毒的行为检测防御引擎，通过分析常见的勒索软件样本，总结了样本具有的共性特征形成了引擎行为库，系统 API 级别分析，有效抵御未知勒索病毒，提供专利级针对未知勒索病毒的诱饵防护引擎，通过自动生成的高仿真文件诱捕未知勒索病毒的攻击，并进行实时阻断。提供此功能证明材料

四、数据库审计系统（1 套）

1.要求设备内存容量不低于 8GB，硬盘容量不低于 2TB，要求网口最低配置不低于 1 管理口+1HA

口+4 审计口（4 个千兆电），要求设备总网络吞吐量不低于 3G，数据库实例授权许可数量：无限。

2.▲要求支持主流数据库的审计。支持 MongoDB、HBase、Hive、Redis、Elasticsearch、Cassandra、HDFS、Impala、Graphbase、Greenplum、Spark SQL、SSDB、ArangoDB、Neo4j、OrientDB 等数据库的审计。提供此功能证明材料。

3.要求支持数据库请求和返回的双向审计，特别是返回结果集和返回字段、执行状态、影响行数、执行时长、客户端工具、主机名等内容，支持通过设置保存行数、最大保存长度来控制返回结果集的大小。

4.▲要求内置安全规则不少于 900 条，如 SQL 注入、缓冲区溢出等，提供此功能证明材料。

5.要求支持安全规则遍历匹配，针对某个操作，将全部安全规则进行匹配，并返回所有匹配的告警结果。

6.▲要求支持日志查询时分析筛选能力，根据查询条件自动分析出存在的数据库账号、客户端 IP、客户端工具、操作系统用户名、服务端 IP、操作类型、数据库名/实例名、表名、主机名、执行状态、执行时长、影响行数等，并支持在以上各个维度中灵活筛选分析。

7.▲要求支持自定义报表，自定义报表支持告警名称、告警等级、操作类型、操作系统用户名、数据库名/实例名、主机名、数据库账号、客户端 IP、客户端工具、数据库类型、客户端端口 11 种统计维度，支持来自审计日志、告警日志、会话日志的 29 种统计指标，根据以上条件进行灵活选择后生成报表，提供此功能证明材料。

8.要求内置运维终端，可实现日志查看与下载、监控日志、设备状态检测、查看系统资源使用、查看共享内存使用、查看 Kafka 消费情况、执行 SQL 语句、执行常用命令、特权运维等。提供此功能证明材料。

五、日志审计系统（1 套）

1. 要求设备最低日志处理能力不低于 2000EPS,峰值不低于 4000EPS,日志源授权不低于 55 个，内存不低于 8G，硬盘不低于 2T，网口不低于 6 个千兆工作管理口。

2. ▲要求采用解决方案包上传对设备进行功能扩展，无需代码开发。提供此功能证明材料。

3.要求支持对 Agent 进行统一管控，包括卸载、升级、启动及停止操作，支持将日志收集策略统一分发。

4.要求内置 5000+解析规则，支持对收集的 5000+设备类型日志进行解析（标准化、归一化），解析维度多达 200+，解析规则可以根据客户要求定制扩展

5.要求支持按日期、时间、设备类型、日志类型、日志来源、威胁值、源地址、目的地址、事件类型、时间范围、操作对象、技术方式、技术动作、技术效果、攻击类型、地理城市等参数进行过滤查询。

6.要求具备安全评估模型，评估模型基于设备故障、认证登录、攻击威胁、可用性、系统脆弱性等纬度加权平均计算总体安全指数。安全评估模型可以显示总体评分、历史评分趋势。安全评估模型各项指标可钻取具体的评分扣分事件。

7.▲要求三维关联分析；支持通过资产、安全知识库、弱点库三个维度分析事件是否存在威胁，并形成关联事件，提供此功能证明材料。

8.通过在目标主机上安装 Agent 程序，支持监测目标主机的 CPU 利用率、内存使用率、硬盘使用率、硬盘使用情况、流量等信息。

9.▲资产拓扑支持按照实际的用户环境进行编辑发布并可以和资产进行绑定，拓扑可以显示资产采集的事件数量被采集资产的状态等信息，

10.▲要求支持分布式部署，支持页面一键添加子节点，自动进行绑定添加，采集器可以选择同步日志范围，按需转发数据，提供此功能证明材料。

六、APT 攻击预警系统（1 套）

1.要求设备 MTBF 不低于 65000 小时，吞吐率不低于网络层 10G，HTTP 最大并发数不低于 20 万/秒，邮件处理数不低于 300 万封/24 小时，文件检测不低于 10 万个/24 小时。内存不低于 8G，硬盘容量不低于 2T。网络接口配置不低于 6 个千兆电口。

2.要求支持解析 HTTP、FTP、SMTP、POP3、SMB、IMAP、DNS、HTTPS、SMTPS、POP3S、IMAPS、RADIUS、KRB5、SNMP、NETFLOW V9、TFTP、NNTP 等协议报文（HTTPS、SMTPS、POP3S、IMAPS 加密协议解析需要导入服务器私钥证书），并提供审计协议类型的端口号配置，可根据需要变更端口号。

3.▲要求支持 GTP、PFCP、NGAP 等 5G 协议解析和审计，支持识别 ORACLE、HTTP、MSSQL、SYBASE、MYSQL、TELNET、FTP、SMTP、POP3、DB2、oscar、dmdb、KINGBASE、PostgreSQL、SMB、IMAP、LDAP、QQ、RADMIN、MONGODB、REDIS、MQTT、AFP、gbase、TIDB、RSYNC、MEMCACHE 等登录行为，提供此功能证明材料。

4.要求支持检测 WEB 攻击、恶意文件攻击、远程控制、WEB 后门访问、WEB 行为分析、DGA 域名请求、SMB 远程溢出攻击、弱口令、拒绝服务攻击、隧道通信、暴力破解、挖矿、扫描行为、漏洞利用、邮件社工攻击、ARP 欺骗、密码明文形式传输等行为。

5.▲要求支持自动对系统告警事件降噪收敛处理，以基于实体的事件分类方式，将 TOP30 异常客户端 IP、安全事件发生次数用不同颜色柱状图排序展示，可一键下钻查看原始告警数量及攻击状态；导出报表支持的枚举信息至少包含客户端 IP、服务端 IP、成功次数、不同风险级别次数、事件次数、事件名称、首次发生时间、最近发生时间等。提供此功能证明材料。

6.要求支持自定义 HTTP 登录行为的用户名获取来源，包括但不限于请求头、URL、Cookie、POST-body；支持自定义配置状态码、返回内容与登录成功/失败状态的绑定关系。

7.要求支持 IP、端口、SMB、Radmin、ICMP、ARP、传输层协议和漏洞扫描行为检测。

8.要求支持从多个维度统计风险告警数量，包括但不限于告警类型、客户端 IP、服务端 IP、威胁情报、告警规则 ID，支持导出 excel 表格，帮助采购人进行告警研判。

9.▲风险查询要求支持一键切换运营模式和专业模式，满足不同场景的研判需求。运营模式可自由选择常用条件，如事件类型、风险级别、攻击状态、规则 ID、回放包 ID、报文、CVE/CNNVD 编号等；专业模式支持多语法组合查询，包含但不限于 AND、OR、NOTIN、IN、==、!=，专业模式包含数据窃取、恶意文件投递、内部横向扩散等 7 种常用查询模版外，支持通过历史筛选条件新增自定义模版，方便后续查询使用，提供此功能证明材料。

10.要求支持攻击链路可视化，一键溯源查看攻击全貌，将攻击者在网络中的活动路径、攻击过程以图形化方式完整的展示出来，帮助用户更好理解攻击者行为。

11.要求具备挖矿专项分析场景，可快速获悉矿机外联通信行为 TOP10、矿池访问次数 TOP10、挖矿软件受害者 TOP10，并可支持域名、多 IP 快速检索，可根据回连次数、矿机 IP、首次发生时间、最近发生时间、回连状态等信息回溯相关挖矿行为的全生命周期活动。

12.要求具备勒索专项分析场景，可快速获悉勒索入侵全流程阶段，迅速定位中招主机 IP、展示受害者 TOP10 和勒索病毒家族分布等关键信息。

13.▲要求含 30 种以上的深度检测模块，可支持 shiro 反序列化、蚁剑、哥斯拉、冰蝎 3.0、冰蝎 4.0 等检测能力,且能识别如 shootback、TunnaProxy、dnscat2、reGeorg、reDuh、CobaltStrike 等隧道通信工具，提供此功能证明材料。

14.要求采用多并发沙箱检测技术，集成主流的操作系统 winXP、win7、win10、linux 等多种检测环境，拥有多项自主研发技术和专利。结合平台内置反病毒引擎和静态分析技术对恶意特征

文件、文件漏洞、未知威胁等深度关联分析。 **七、等保测评服务（1 系统）** 1. ▲要求提供一个业务系统的二级系统等级保护测评服务。并提供最终的测评报告及证书。 **八、防火墙维保服务（2 年）** 1.▲要求包含基本网络防火墙功能、访问控制功能、攻击防护、Web 防护、用户认证功能、链路负载均衡功能、流量控制、资产识别、IPSec VPN 等授权功能。提供明御防火墙 DAS-TGFW 原厂商硬件质保服务、软件平台升级、特征库升级和 7*24 小时技术支持服务。维保服务期二年。 2、▲设备出现部件故障更换部件，出现整机故障更换整机。硬件故障发生后需于 24 小时内解决故障。 **九、柜式七氟丙烷气体灭火装置（1 套）** 1.配置泄压口，配置 4 个点型感温火灾探测器，配置点型光电感烟火灾探测器，配置气体释放报警器，配置气体灭火系统控制装置，配置输入/输出模块。满足消防要求。
备注：标“▲”为重要参数，其他为一般参数。